Hosted Email Security

Guide de l'administrateur

Protection de la messagerie contre les menaces intégrée dans un service hébergé

Trend Micro Incorporated se réserve le droit de modifier sans préavis ce document et Hosted Email Security décrits dans ce document. Avant d'installer et d'utiliser Hosted Email Security, veuillez lire les fichiers lisez-moi, les notes de publication et/ou la dernière version de la documentation destinée à la documentation applicable, disponibles sur le site Web de Trend Micro à l'adresse :

http://docs.trendmicro.com/fr-fr/smb/hosted-email-security.aspx

Trend Micro et le logo t-ball de Trend Micro sont des marques commerciales ou déposées de Trend Micro, Incorporated. Tous les autres noms de produit ou de société peuvent être des marques commerciales ou des marques déposées de leurs propriétaires.

Copyright © 2013. Trend Micro Incorporated. Tous droits réservés.

Partie de document n° : HSFM15997/130719

Date de publication : septembre 2013

Protégé par les brevets américains n°5,623,600 ; 5,951,698 ; 5,983,348 ; 6,272,641

Cette documentation présente les principales caractéristiques de Hosted Email Security et/ou fournit des instructions d'installation pour un environnement de production. Lisez la documentation avant d'installer ou d'utiliser Hosted Email Security.

Vous trouverez des informations détaillées sur l'utilisation de fonctions spécifiques de Hosted Email Security dans l'aide en ligne de Trend Micro et/ou la base de connaissances Trend Micro sur le site Web de Trend Micro.

Nous nous efforçons constamment d'améliorer la documentation. Si vous avez des questions, des commentaires ou des suggestions à propos du présent document ou de tout autre document Trend Micro, veuillez nous écrire à docs@trendmicro.com.

Évaluez cette documentation sur le site suivant :

http://www.trendmicro.com/download/documentation/rating.asp

Contenu

Préface

Nouveautés viii

Hosted Email Security Documentation ix
Public cible x
Nomenclatures du document x

Chapitre 1 : Présentation de Trend Micro Hosted Email Security

À propos de Hosted Email Security 1-2
Service supplémentaire Email Encryption 1-2
Hosted Email Security Flux des messages 1-3
Niveaux de protection 1-4
Filtrage basé sur la réputation au niveau de la connexion à la messagerie 1-4
Filtrage basé sur le contenu du message 1-4
Configuration minimale requise 1-5
Logiciel requis pour accéder à votre compte 1-5
Réseau sur site 1-5
Paramètres Hosted Email Security par défaut 1-5

Chapitre 2 : Utilisation de Hosted Email Security

Démarrage 2-2
Enregistrement et activation de Hosted Email Security 2-2
Envoi des informations d'activation de compte 2-3
Obtention d'une clé d'enregistrement et d'un code d'activation 2-3
Activation du service Hosted Email Security 2-4
Redirection de votre enregistrement MX 2-5
Configuration de votre agent de transfert de messages (ATM) 2-6
Activation du filtrage sortant 2-6

Désactivation de Hosted Email Security 2-9
Connexion à la console d'administration 2-9
Première connexion 2-9
Utilisation de la console Web Hosted Email Security 2-11
Rapports 2-11
Onglet Trafic 2-13
Onglet Taille 2-16
Onglet Menaces 2-18
Onglet Détails 2-20
Onglet Spam principal 2-25
Onglet Virus principaux 2-26

Chapitre 3 : Gestion des stratégies

Vue d'ensemble des stratégies 3-2
Paramètres de stratégie par défaut 3-3
Filtrage de contenu 3-6
Filtrage de contenu par mot-clé 3-6
Filtrage de contenu à l'aide des expressions régulières 3-9
Pondération des listes d'expressions à mot-clé 3-12
Actions de règle 3-13
Supprimer le message entier 3-13
Envoyer le message maintenant 3-14
Mettre le message en quarantaine 3-15
Nettoyer les virus nettoyables et supprimer ceux qui ne peuvent pas être nettoyés 3-16
Supprimer les pièces jointes correspondantes 3-16
Insérer un horodatage dans le corps du message 3-17
Baliser la ligne d'objet 3-17
Envoyer un message de notification 3-18
Copier en copie cachée (BCC) un autre destinataire 3-19
Rejeter le message 3-20
Contourner une règle 3-20
Chiffrer des e-mails 3-21
Lecture d'un e-mail chiffré 3-22
Ordre d'exécution des règles 3-26
Actions Intercepter 3-26
Remarque importante sur l'action Envoyer maintenant 3-26

Actions Modifier 3-27
Actions Surveiller 3-27
Limitations de scan 3-27
Action Chiffrement d'e-mail 3-28
Ajout et modification de règles 3-28
Ajout d'une nouvelle règle 3-28
Modification d'une règle existante 3-36
Copie d'une règle existante 3-38
Suppression d'une règle existante 3-38

Chapitre 4 : Expéditeurs approuvés, quarantaine et journaux

Expéditeurs approuvés 4-2
Quarantaine 4-3
Demande de mise en quarantaine 4-3
Paramètres de l'option Mettre en quarantaine 4-4
Approbation de messages ou d'expéditeurs depuis l'e-mail d'aperçu des spams (action en ligne) 4-4
Web End-User Quarantine 4-13
Réinitialisation du mot de passe de l'utilisateur final 4-13
Journaux 4-14
Détails sur le suivi des messages 4-15

Chapitre 5 : Administration et réputation IP

Paramètres de réputation IP 5-2
Utilisation du curseur dynamique de réputation 5-3
Réglage des paramètres d'exclusion IP 5-4
Section d'exclusion IP 5-4
Serveurs de messagerie valides 5-5
Sélection des listes de réputation IP standard 5-5
Listes de réputation IP Approuvés et Bloqués 5-7
Bloquer tous les pays sauf 5-8
Dépannage des paramètres de réputation IP 5-10
Administration 5-11
Modification des mots de passe 5-11
Modification du mot de passe administrateur 5-12
Réinitialisation d'un mot de passe pour Web EUQ 5-13

Gestion des répertoires 5-13
Remarques sur la gestion des répertoires 5-14
Vérification de votre répertoire d'utilisateurs 5-16
Gestion des domaines 5-17
À propos de l'état du domaine 5-17
Ajout d'un domaine 5-18
Confirmation de l'envoi des messages par le service 5-20
Modification d'un domaine 5-20
Reprendre les domaines suspendus 5-22
Comarquage 5-22
Spécifications du logo 5-22
Comarquage de la console d'administration 5-23
Comarquage de l'interface Web EUQ 5-24
Accès à un site comarqué 5-27
Services Web 5-29
Téléchargement du Guide des services Web Hosted Email Security .. 5-30
Afficher le contrat de niveau de service 5-31
Gestion à distance 5-33
Modes de licence 5-35

Annexe A : Foire Aux Questions

Qu'est-ce que Trend Micro™ Hosted Email Security ? A-1
Quels sont les avantages d'un service hébergé de sécurité de messagerie ? A-1
Ai-je besoin d'acheter/de mettre à niveau du matériel ou des logiciels ? A-2
Combien coûte le service ? A-2
Quel est le niveau de confidentialité de ce service ? A-2
Pourquoi devrais-je faire confiance à Trend Micro pour la gestion de ma messagerie ? A-2
De quoi ai-je besoin pour utiliser ce service ? A-3
Comment commencer à utiliser ce service ? A-3
Comment rediriger mes e-mails/mon enregistrement Mail eXchange ? A-3
Comment accepter les messages provenant du service ? A-3
Pourquoi mon domaine garde-t-il l'état Vérification ? A-4
Puis-je essayer le service sur un nombre limité d'utilisateurs ? A-4

La remise de mes e-mails va-t-elle être retardée par l'utilisation de ce service ? A-4
Trend Micro stocke-t-il/archive-t-il les e-mails ? A-4
Comment réinitialiser ou renvoyer un mot de passe d'utilisateur final pour Web EUQ ? A-4
Qu'arrive-t-il à mes messages si mon serveur de messagerie est indisponible pendant un certain temps ? A-5
Où est acheminé mon courrier sortant ? A-5
Les revendeurs et les clients finaux peuvent-ils se connecter à l'aide des informations de connexion existantes ? A-5
Comment puis-je modifier un nom de domaine géré ? A-5
Comment puis-je utiliser la fonctionnalité de message test ? A-6
Pourquoi l'écran Gestion de domaine est-il désactivé ? A-6
Que se passe-t-il lorsque ma licence arrive à expiration ? A-6

Annexe B : Informations de contact et ressources Internet

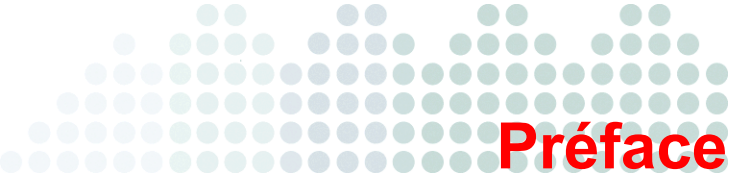
Contacter l'assistance technique B-2
Informations de contact générales B-3
Disponibilité du service B-3
Remise d'e-mails B-3
Base de connaissances B-4
Soumission de code suspect à Trend Micro B-4
TrendLabs B-7
Centre d'informations de sécurité B-7

Annexe C : Présentation de Web EUQ

Accès au service Web End User Quarantine C-2
Création d'un compte C-2
Connexion à Hosted Email Security Web End-User Quarantine C-4
Traitement des spams en quarantaine C-4
Utilisation de l'écran Expéditeurs approuvés C-6
Modification du mot de passe C-8

Glossaire

Index



Préface

Bienvenu dans le *Guide de l'administrateur Trend Micro™ Hosted Email Security*.
Ce document contient des informations sur les paramètres et les niveaux de service.

Sujets abordés dans cette préface :

- *Nouveautés* à la page viii
- *Hosted Email Security Documentation* à la page ix
- *Public cible* à la page x
- *Nomenclatures du document* à la page x

Nouveautés

Les nouvelles fonctions ajoutées à Trend Micro Hosted Email Security sont les suivantes :

- Intelligentes Weiterleiten von E-Mails und Außerkraftsetzen von Domains (Juli 2013) – siehe Seite page 5-17.
- Integration mit Trend Micro Licensing Management Platform (Februar 2013) – für weitere Informationen siehe Online-Hilfe (http://docs.trendmicro.com/all/smb/hes/vAll/de-de/help/licensing_management_platform.htm).
- Möglichkeit, mehr als einen Host als Ziel- oder Postausgangsserver hinzuzufügen (November 2012) – siehe Seite page 5-17.
- Détails (des événements) dans les journaux de suivi des messages (juin 2012) – voir page 4-15.

Hosted Email Security Documentation

La documentation de Trend Micro™ Hosted Email Security comprend les éléments suivants :

Aide en ligne : vous aide à configurer toutes les fonctions par le biais de l'interface utilisateur. Vous pouvez accéder à l'aide en ligne en ouvrant la console Web et en cliquant sur l'icône d'aide ( ).

Guide de l'administrateur : ce guide vous aide à configurer tous les paramètres du service.

Remarque : Dans la version publiée le 15 mars 2010, le service « InterScan Messaging Hosted Security » devient « Hosted Email Security ».

Guide des services Web : vous aide à automatiser les tâches administratives de Hosted Email Security.

Guide du service Web EUQ (End User Quarantine) pour l'utilisateur final : vous explique comment gérer les messages de spam mis en quarantaine à l'aide du service Web End User Quarantine de Trend Micro.

Le *Guide de l'administrateur* et le *Guide du service Web EUQ* sont disponibles à l'adresse :

http://fr.trendmicro.com/fr/products/enterprise/hosted-email-security/support/index.html

Public cible

La documentation s'adresse aux responsables informatiques et aux administrateurs de messagerie. La documentation considère que le lecteur dispose de connaissances approfondies sur les réseaux de messagerie électronique, y compris des informations sur les éléments suivants :

- Le protocole SMTP
- Les agents de transfert de messages (ATM)

La documentation ne considère pas que le lecteur dispose de connaissances sur la technologie antivirus ou anti-spam.

Nomenclatures du document

Pour vous aider à localiser et à interpréter facilement les informations, cette documentation utilise les nomenclatures suivantes.

NOMENCLATURE	DESCRIPTION
MAJUSCULES	Acronymes, abréviations, noms de certaines commandes et touches sur le clavier
Gras	Menus et commandes de menus, boutons de commande, onglets, options et tâches ScanMail
Italique	Références à d'autres documents
`Police monospace`	Exemples, exemples de lignes de commande, code du programme, noms de fichier et rendu du programme
Remarque :	Remarques de configuration
Conseil :	Recommandations
AVERTISSEMENT !	Rappels sur des actions ou configurations qui devraient être évitées

Chapitre 1

Présentation de Trend Micro Hosted Email Security

Trend Micro™ Hosted Email Security fournit des services de sécurité hébergés hautement performants et rentables afin de protéger les entreprises contre les spams, les virus et le contenu inapproprié avant qu'ils ne pénètrent votre réseau.

Sujets abordés dans ce chapitre :

- *À propos de Hosted Email Security* à la page 1-2
- *Hosted Email Security Flux des messages* à la page 1-3
- *Configuration minimale requise* à la page 1-5
- *Paramètres Hosted Email Security par défaut* à la page 1-5

À propos de Hosted Email Security

Hosted Email Security offre des fonctions de gestion puissantes, qui vous permettent de personnaliser vos défenses contre les menaces et de configurer des stratégies d'utilisation de la messagerie adaptées aux besoins de votre entreprise. Parmi les fonctions propres à ce niveau de service :

- Filtrage personnalisé des menaces, filtrage des e-mails sortants (optionnel)
- Fonctions de filtrage du contenu
- Email Encryption (uniquement proposé sous forme de supplément disponible séparément)

Service supplémentaire Email Encryption

Trend Micro Email Encryption pour les messages sortants est un supplément accessible aux utilisateurs de Hosted Email Security. Email Encryption s'intègre parfaitement aux fonctions de filtrage de contenu de Hosted Email Security. Le service ne chiffre pas automatiquement les messages. Une fois activé, Email Encryption s'affiche comme une option de règle au sein de la console d'administration Hosted Email Security. Vous devrez configurer les règles d'application du chiffrement dans le cadre de la règle. Consultez la rubrique *Chiffrer des e-mails* à la page 3-21 pour connaître la marche à suivre pour la création des règles permettant d'appliquer le chiffrement.

Pour utiliser le service Email Encryption, vous devez d'abord déployer le filtrage sortant sur Hosted Email Security.

Hosted Email Security Flux des messages

La *Figure 1-1* montre le flux du trafic des messages à partir d'Internet, à travers les serveurs Hosted Email Security, puis sur votre serveur de messagerie.

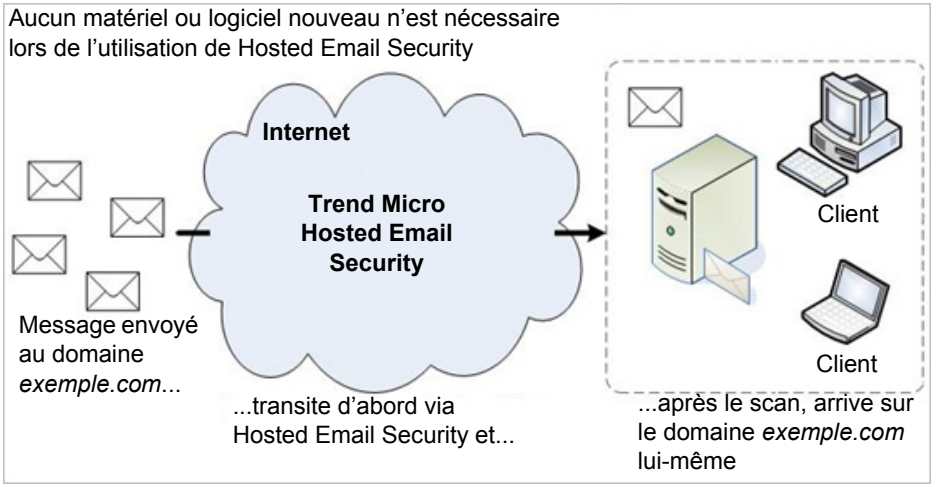

Aucun matériel ou logiciel nouveau n'est nécessaire lors de l'utilisation de Hosted Email Security
Internet
Trend Micro Hosted Email Security
Client
Client
Message envoyé au domaine *exemple.com*...
...transite d'abord via Hosted Email Security et...
...après le scan, arrive sur le domaine *exemple.com* lui-même

FIGURE 1-1 Hosted Email Security diagramme du déroulement des opérations

Hosted Email Security effectue les opérations suivantes :

1. Le serveur de messagerie d'origine réalise une recherche DNS pour déterminer l'emplacement du domaine exemple.com. L'enregistrement Mail eXchange (MX) d'exemple.com contient l'adresse IP de Hosted Email Security au lieu de l'adresse IP initiale d'exemple.com, car Hosted Email Security doit d'abord scanner le courrier de votre entreprise avant sa remise finale à votre serveur local de messagerie.
2. Le serveur de messagerie initial achemine le courrier vers Hosted Email Security.
3. Les serveurs Hosted Email Security acceptent le message et réalisent pour vous le filtrage des messages et la correspondance des stratégies.
4. Si un message est listé pour être livré en fonction de sa stratégie de sécurité ou son état de validité, les serveurs Hosted Email Security acheminent le message vers les serveurs de messagerie initiaux d'exemple.com.

Niveaux de protection

Hosted Email Security propose deux niveaux de protection. Ils comprennent :

- Un filtrage basé sur la réputation au niveau de la connexion à la messagerie
- Filtrage basé sur le contenu du message

Filtrage basé sur la réputation au niveau de la connexion à la messagerie

Lorsqu'un serveur de messagerie ascendant essaie de se connecter à un serveur Hosted Email Security, le serveur Hosted Email Security lance une requête auprès des services de réputation de messagerie (Email Reputation Services, ERS) de Trend Micro pour déterminer si l'adresse IP de l'expéditeur qui se connecte est digne de confiance. Hosted Email Security réalise un premier niveau de filtrage avant de recevoir le message lui-même ; c'est ainsi que le contenu du message n'est jamais scanné.

Si l'adresse IP de l'expéditeur est une source connue de spam, l'adresse IP du serveur de l'expéditeur est marquée comme indigne de confiance. Hosted Email Security rejette la tentative de connexion de la part de cette adresse IP.

Si l'ordinateur de l'expéditeur fait partie d'un réseau de zombies ou est un PC zombie, l'adresse IP se trouvera dans la base de données dynamique ERS (Email Reputation Services) qui identifie les sources de spam dès qu'elles apparaissent et pendant toute la durée de leur activité. Hosted Email Security informera le serveur de l'expéditeur que Hosted Email Security est temporairement indisponible. S'il s'agit d'un serveur légitime, il tentera de nouveau ultérieurement.

Filtrage basé sur le contenu du message

Après que le message a passé le premier niveau de protection, Hosted Email Security applique le filtrage de contenu grâce à deux moteurs d'analyse :

- Spam et phishing
- Programmes malveillants (virus, programmes espions, etc.)

Plusieurs technologies sont exploitées dans ces moteurs d'analyse, à savoir :

- Fichiers de signatures (ou signatures de spam)
- Règles heuristiques
- Apprentissage par la machine (filtrage statistique)
- Réputation d'URL

Hosted Email Security examine le contenu du message afin de déterminer s'il contient des programmes malveillants tels que des virus ou bien s'il s'agit de spams, etc., en fonction des stratégies basées sur le contenu de ce message.

Configuration minimale requise

Hosted Email Security ne requiert aucun matériel supplémentaire (autre que votre passerelle de messagerie) dans vos locaux. Tout le matériel de scan se situe hors site, dans les centres d'exploitation de réseau de Trend Micro. Pour accéder à votre compte en ligne administrateur Hosted Email Security, vous avez besoin d'un ordinateur personnel avec accès à Internet.

Logiciel requis pour accéder à votre compte

L'utilisation de la console Web de Hosted Email Security requiert Java Script™. Hosted Email Security prend en charge les navigateurs suivants pour la console Web :

- Microsoft™ Internet Explorer™ 6.0 et 7.0
- Mozilla™ Firefox™ 2.0

Réseau sur site

Les éléments suivants sont requis avant de pouvoir activer Hosted Email Security :

- Une passerelle Internet ou une connexion SMTP de groupe de travail existante.
- Un accès à l'enregistrement Mail eXchange du DNS pour rediriger l'enregistrement hébergé de messagerie MX. (Si besoin est, contactez votre fournisseur d'accès pour plus d'informations ou une aide à la configuration.)

Remarque : Ne redirigez pas votre enregistrement MX avant d'avoir reçu la confirmation que votre compte a été créé. Si vous redirigez votre enregistrement MX avant la création du compte, votre courrier sera perdu. Les informations de redirection seront fournies par Trend Micro.

Paramètres Hosted Email Security par défaut

Pour assurer un service continu et de haute qualité et pour protéger votre réseau contre les attaques SMTP courantes, telles que la saturation de la messagerie et les attaques « Zip of Death », les restrictions par défaut du service comprennent :

- Limitations de taille des messages : 50 Mo par message

- Nombre total de couches incorporées dans un fichier compressé : 20 couches
- Volume total d'un message décompressé : 30 Mo
- Nombre total de fichiers dans une archive compressée : 353 fichiers
- Volume total de stockage en quarantaine par poste : 50 Mo
- Nombre total d’entrées d’expéditeurs approuvés par poste : 50

Chapitre 2

Utilisation de Hosted Email Security

Ce chapitre présente les notions de base sur l'accès à la console d'administration Hosted Email Security et son utilisation, et explique les rapports disponibles à partir de la console.

Sujets abordés dans ce chapitre :

- *Démarrage* à la page 2-2
- *Connexion à la console d'administration* à la page 2-9
- *Utilisation de la console Web Hosted Email Security* à la page 2-11
- *Rapports* à la page 2-11

Démarrage

Hosted Email Security doit être configuré pour fonctionner correctement et efficacement. Ce processus de configuration comprend les étapes suivantes :

TABLEAU 2-1. Liste de contrôle de configuration de Hosted Email Security

ÉTAPE	POUR PLUS D'INFORMATIONS	
1. Envoyez les informations d'activation de votre compte	*Envoi des informations d'activation de compte* à la page 2-3	❑
2. Connectez-vous à la console d'administration Web	*Première connexion* à la page 2-9	❑
3. Ajoutez un ou plusieurs domaines à gérer	*Gestion des domaines* à la page 5-17	❑
4. Confirmez l'envoi des messages par Hosted Email Security	*Confirmation de l'envoi des messages par le service* à la page 5-20	❑
5. Redirigez l'enregistrement MX de votre domaine	*Redirection de votre enregistrement MX* à la page 2-5	❑
6. Configurez votre ATM, le cas échéant	*Configuration de votre agent de transfert de messages (ATM)* à la page 2-6	❑

Enregistrement et activation de Hosted Email Security

Vous devez disposer d'un code d'activation (Activation Code ou AC) ou d'une clé d'enregistrement (Registration Key ou RK) pour l'activation. Si vous n'avez ni code d'activation, ni clé d'enregistrement, contactez votre représentant commercial Trend Micro. Tant que vous n'aurez pas saisi un code d'activation valide, vous ne pourrez pas utiliser Hosted Email Security.

Vous devez enregistrer votre service avant de l'utiliser. Vous pouvez procéder à l'enregistrement en ligne à l'adresse suivante :

https://olr.trendmicro.com/registration/eu/fr/login.aspx

Le service Email Encryption est un complément de Hosted Email Security. Il est donc disponible séparément.

Envoi des informations d'activation de compte

Avant d'utiliser Hosted Email Security, vous devez activer le compte.

Pour activer le compte Hosted Email Security :

1. Retrouvez votre confirmation d'achat et la clé d'enregistrement dans l'e-mail envoyé par Trend Micro.
2. Consultez le site d'enregistrement en ligne de Trend Micro (URL fourni dans l'e-mail), choisissez un nom d'utilisateur et un mot de passe et achevez le processus d'enregistrement.
3. Trend Micro vous envoie un e-mail avec le nom d'utilisateur que vous avez choisi et l'URL de la console d'administration Hosted Email Security.
4. Connectez-vous à la console avec ce nom d'utilisateur. Vous êtes invité à entrer les informations de domaine et d'adresse IP.
5. Cliquez sur **Envoyer**. Trend Micro crée votre compte et vous envoie un e-mail de confirmation. (Prévoyez un délai de 24 à 48 heures.) Cet e-mail contient les informations sur la redirection de votre enregistrement MX.
6. Envoyez un e-mail à votre adresse électronique test pour vérifier que les e-mails peuvent transiter via Hosted Email Security.
7. Redirigez votre enregistrement MX en suivant les instructions de l'e-mail mentionné ci-avant.

Remarque : Ne redirigez pas votre enregistrement MX avant d'avoir reçu la confirmation que votre compte a été créé. Si vous redirigez votre enregistrement MX avant la création du compte, votre courrier sera perdu.

Obtention d'une clé d'enregistrement et d'un code d'activation

Clé d'enregistrement

Les clients situés en Amérique du Nord, en Europe, au Moyen-Orient et en Afrique ont besoin d'une clé d'enregistrement pour enregistrer Hosted Email Security. Celle-ci utilise 22 caractères, tirets compris, au format suivant :

```
XX-XXXX-XXXX-XXXX-XXXX
```

Les clients des régions mentionnées ci-dessus doivent enregistrer Hosted Email Security au moyen de leur clé d'enregistrement avant de recevoir un code d'activation qui leur permettra de commencer à utiliser le service.

Code d'activation

Le code d'activation est obligatoire pour tous les clients. La console Web affiche l'état de votre licence. Un code d'activation utilise 37 caractères, tirets compris, au format suivant :

`XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`

Une fois Hosted Email Security enregistré, Trend Micro vous envoie votre code d'activation.

Activation du service Hosted Email Security

Lors de la première installation de Hosted Email Security, le premier écran qui s'affiche est intitulé Activation du service, comme illustré dans la *figure 2-1*. Dans cet écran, indiquez les domaines à gérer via le service Hosted Email Security.

Remarque : Hosted Email Security doit posséder un enregistrement des domaines de votre société pour appliquer les paramètres de réputation IP aux messages qui lui parviennent.

Pour ajouter un domaine à gérer avec Hosted Email Security :

1. Saisissez les informations suivantes dans les champs prévus à cet effet (les champs obligatoires sont affichés en gras) :
   - Le nouveau **nom de domaine**
   - **L'adresse IP ou le nom de domaine complet** (fully qualified domain name, FQDN)
   - **Le numéro de port** du serveur de messagerie du domaine
   - Le nombre de **postes assignés** à ce domaine
   - L'adresse électronique test (utilisez cette adresse électronique comme destinataire d'un message test pour confirmer l'envoi par Hosted Email Security.)
2. Sélectionnez **Activer le filtrage sortant**, puis indiquez l'adresse IP du (des) serveur(s) sortant(s).

3. Cliquez sur **Activer le domaine.** Le domaine s'affiche dans le tableau Domaines en bas de l'écran.
4. Cliquez sur **Envoyer**. Si le domaine est valide et qu'il existe un enregistrement MX pour celui-ci, le nouveau domaine, l'adresse IP ou le nom de domaine complet, le numéro de port, les postes assignés et d'autres informations s'affichent dans le tableau Domaine en bas de l'écran et Trend Micro envoie un message électronique de bienvenue à l'adresse d'administration enregistrée.

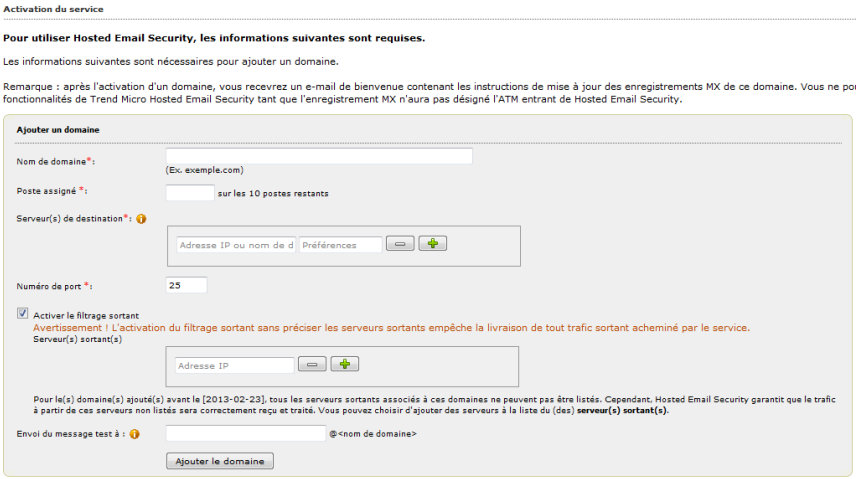

Activation du service
Pour utiliser Hosted Email Security, les informations suivantes sont requises.
Les informations suivantes sont nécessaires pour ajouter un domaine.
Remarque : après l'activation d'un domaine, vous recevrez un e-mail de bienvenue contenant les instructions de mise à jour des enregistrements MX de ce domaine. Vous ne po
fonctionnalités de Trend Micro Hosted Email Security tant que l'enregistrement MX n'aura pas désigné l'ATM entrant de Hosted Email Security.
Ajouter un domaine
Nom de domaine*:
(Ex. exemple.com)
Poste assigné *:
sur les 10 postes restants
Serveur(s) de destination*:
Adresse IP ou nom de d
Préférences
Numéro de port *:
25
Activer le filtrage sortant
Avertissement ! L'activation du filtrage sortant sans préciser les serveurs sortants empêche la livraison de tout trafic sortant acheminé par le service.
Serveur(s) sortant(s)
Adresse IP
Pour le(s) domaine(s) ajouté(s) avant le [2013-02-23], tous les serveurs sortants associés à ces domaines ne peuvent pas être listés. Cependant, Hosted Email Security garantit que le trafic
à partir de ces serveurs non listés sera correctement reçu et traité. Vous pouvez choisir d'ajouter des serveurs à la liste du (des) serveur(s) sortant(s).
Envoi du message test à :
@<nom de domaine>
Ajouter le domaine

FIGURE 2-1. Écran Activation du service

Redirection de votre enregistrement MX

L'enregistrement Mail eXchange (MX) détermine l'acheminement des messages pour tous les e-mails envoyés à votre domaine. Pour acheminer les messages destinés à votre domaine par le biais des serveurs Hosted Email Security, vous devez rediriger votre enregistrement MX. L'e-mail de bienvenue que vous recevez vous indique l'emplacement vers lequel rediriger votre enregistrement MX.

Pour rediriger l'enregistrement MX, remplacez votre enregistrement MX actuel par celui fourni dans l'e-mail de bienvenue que Trend Micro vous a envoyé après votre enregistrement. Vous pouvez effectuer cette modification manuellement (petits comptes auto-gérés) ou faire appel à un technicien du service d'assistance.

Si vous avez besoin d'aide pour configurer les enregistrements MX pour votre domaine, contactez votre fournisseur d'accès Internet ou votre technicien DNS (Domain Name Service).

Remarque : La propagation DNS peut prendre jusqu'à 48 heures. Pendant ce délai, ne désactivez pas la sécurité sur site. Il est possible que vous receviez des e-mails directement pendant une courte période, jusqu'à ce que la transition soit terminée.

Configuration de votre agent de transfert de messages (ATM)

Pour tous les clients Hosted Email Security, les messages de type « spam ou phishing » sont supprimés par défaut. Les utilisateurs de la version complète peuvent modifier cette règle. (Voir *Modification d'une règle existante* à la page 3-36.)

Vous pouvez choisir de configurer votre ATM pour qu'il gère les spams en fonction de la stratégie de sécurité de votre entreprise. Les messages contenant une balise peuvent être réexpédiés dans un dossier de spam, être supprimés ou envoyés à l'utilisateur final, etc. Si vous optez pour le balisage de ces messages, la balise **Spam/Phishing>** est ajoutée à la ligne d'objet des spams, suivie de la ligne d'objet initiale.

Remarque : Ce document n'a pas pour vocation de fournir des instructions détaillées sur la configuration ATM. Veuillez contacter votre gestionnaire de messagerie si vous avez besoin d'aide.

Activation du filtrage sortant

Trend Micro Email Encryption est uniquement proposé sous forme de supplément pour Hosted Email Security avec filtrage sortant. Le filtrage sortant est disponible sans frais supplémentaires.

Si vous ne disposez pas d'un compte d'enregistrement en ligne (OLR) Trend Micro, vous devez contacter l'assistance technique Trend Micro pour activer cette fonction. Si vous disposez d'un compte OLR, vous pouvez le faire depuis la console d'administration de Hosted Email Security.

Si vous disposez d'un compte d'enregistrement en ligne

Avec un compte d'enregistrement en ligne (OLR), l'activation du filtrage sortant est simple.

Pour activer le filtrage sortant :

1. Dans le menu de gauche, sélectionnez **Administration > Gestion de domaine** pour ouvrir l'écran Gestion de domaine.
2. Dans le tableau Domaines en bas de l'écran, cliquez sur le lien hypertexte du nom de domaine pour lequel vous voulez activer le filtrage sortant. L'écran **Gestion de domaine > {nom-de-votre-domaine}** apparaît. Ses champs ont été pré-renseignés au moyen des informations enregistrées pour ce domaine.
3. Sélectionnez **Activer le filtrage sortant**.
4. Spécifiez au moins un **serveur sortant** en utilisant son adresse IP.
5. Cliquez sur **Enregistrer**. Hosted Email Security démarre le processus d'activation du filtrage sortant pour ce domaine. L'état du domaine passe à « Modification ».

Conseil : Après avoir cliqué sur **Enregistrer**, le processus d'activation démarre. Celui-ci peut nécessiter jusqu'à 2 heures pour s'effectuer. Une fois le processus terminé, l'état du domaine affiché par Hosted Email Security passe de Modification « à » « Activé ».

Si vous ne disposez pas d'un compte d'enregistrement en ligne

Le filtrage sortant est une fonction nécessitant un contact avec l'équipe de Trend Micro. Si le filtrage sortant a été paramétré pour votre compte, votre entreprise aura reçu la confirmation par e-mail de Trend Micro indiquant que cette fonction a été activée et vous précisant le serveur concerné par le relais.

Avant de contacter l'assistance technique Trend Micro pour configurer le filtrage sortant, vous devez fournir les informations suivantes :

- Nom de compte
- Nom de domaine et adresse électronique valide sous le domaine

- Votre nom
- Votre adresse électronique
- Adresse IP du serveur de messagerie sortant

L'équipe Trend Micro apportera les modifications nécessaires pour que votre flux de messages sortants soit filtré à travers Hosted Email Security et, lorsqu'il sera prêt, vous en serez informé par e-mail. Vous recevrez ensuite d'autres instructions pour rediriger vos messages sortants vers les serveurs de messagerie sortants Hosted Email Security.

Pour plus d'informations sur l'activation du filtrage sortant ou pour obtenir le service de filtrage sortant, contactez l'assistance technique Trend Micro.

Vérification du filtrage sortant

Lorsque l'assistance technique Trend Micro a fini d'activer le filtrage sortant pour votre compte, vous en êtres informé par e-mail. Consultez l'écran **Administration > Gestion de domaine** pour vérifier que le filtrage sortant est activé, comme le montre la *Figure 2-2* à la page 2-8.

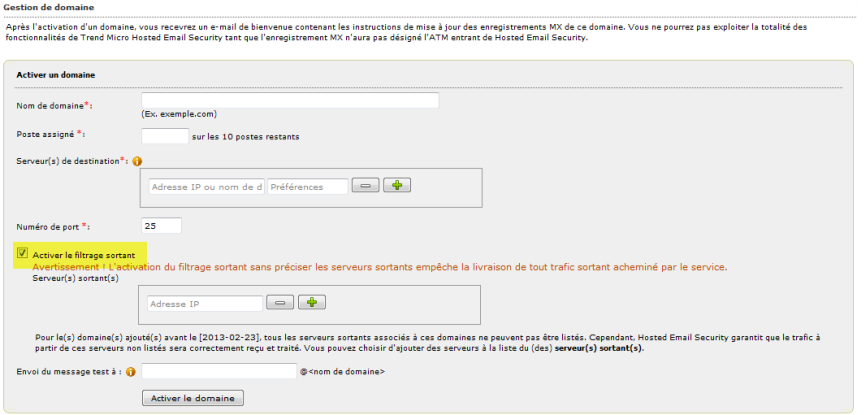

Gestion de domaine
Après l'activation d'un domaine, vous recevrez un e-mail de bienvenue contenant les instructions de mise à jour des enregistrements MX de ce domaine. Vous ne pourrez pas exploiter la totalité des fonctionnalités de Trend Micro Hosted Email Security tant que l'enregistrement MX n'aura pas désigné l'ATM entrant de Hosted Email Security.
Activer un domaine
Nom de domaine*:
(Ex. exemple.com)
Poste assigné *:
sur les 10 postes restants
Serveur(s) de destination*:
Adresse IP ou nom de d
Préférences
Numéro de port *:
25
Activer le filtrage sortant
Avertissement ! L'activation du filtrage sortant sans préciser les serveurs sortants empêche la livraison de tout trafic sortant acheminé par le service.
Serveur(s) sortant(s)
Adresse IP
Pour le(s) domaine(s) ajouté(s) avant le [2013-02-23], tous les serveurs sortants associés à ces domaines ne peuvent pas être listés. Cependant, Hosted Email Security garantit que le trafic à partir de ces serveurs non listés sera correctement reçu et traité. Vous pouvez choisir d'ajouter des serveurs à la liste du (des) serveur(s) sortant(s).
Envoi du message test à :
@<nom de domaine>
Activer le domaine

FIGURE 2-2. Écran Gestion de domaine pour vérifier que « Filtrage sortant » est activé

Achat d'Email Encryption

Pour acheter Email Encryption, vous devez disposer de Hosted Email Security avec filtrage sortant. Vous pouvez tester gratuitement Email Encryption pendant la période

d'évaluation de Hosted Email Security mais vous ne pourrez pas acheter Email Encryption avant de vous être procuré Hosted Email Security et d'avoir activé le filtrage sortant.

Remarque : Dans certaines régions, vous devez obtenir une clé d'enregistrement avant de recevoir un code d'activation. Si vous disposez d'une clé d'enregistrement mais que vous n'avez pas encore de code d'activation, inscrivez-vous en ligne sur le site d'enregistrement en ligne de Trend Micro pour demander votre code : https://olr.trendmicro.com/registration

Désactivation de Hosted Email Security

Pour désactiver Hosted Email Security, vous devez suivre le même processus que lors de l'initialisation du service, et rediriger votre enregistrement MX pour acheminer tout le trafic SMTP entrant vers votre propre serveur de messagerie. Consultez la rubrique *Redirection de votre enregistrement MX* à la page 2-5.

Connexion à la console d'administration

En vous connectant à la console Web Hosted Email Security, vous pouvez visualiser des rapports et utiliser l'outil de suivi des messages pour les localiser. En tant qu'utilisateur de Hosted Email Security (version complète), vous pouvez aussi apporter des modifications à votre stratégie de sécurité de la messagerie.

Première connexion

Le kit de bienvenue (Welcome Packet) que vous avez reçu à la suite de votre inscription à Hosted Email Security contient le nom d'utilisateur et le mot de passe à utiliser lors de votre Première connexion.

Pour vous connecter à la console :

1. Dans votre navigateur, ouvrez l'URL fourni dans l'e-mail de confirmation que vous avez reçu (voir l'*Étape 2* à la page 2-3) pour accéder à la page de connexion.

Hosted Email Security
Powered By TREND
TREND MICRO
Hosted Email Security
Saisissez votre nom d'utilisateur et votre mot de passe pour accéder à la console d'administration.
Connectez-vous avec le nom d'utilisateur et le mot de passe d'enregistrement en ligne Trend Micro. Qu'est-ce que c'est ?
Nom d'utilisateur :
Mot de passe :
Connexion
Vous avez oublié votre mot de passe ?
Vous n'êtes pas abonné à ce service ? Cliquez ici pour découvrir comment vous inscrire dès aujourd'hui.

FIGURE 2-3. Écran de connexion Hosted Email Security

2. Si vous disposez d'un compte d'enregistrement en ligne Trend Micro, sélectionnez **Se connecter avec un nom d'utilisateur et un mot de passe d'enregistrement en ligne Trend Micro.**
3. Entrez votre **nom d'utilisateur** et votre **mot de passe**.
4. Cliquez sur **Connexion**.

Conseil : Après vous être connecté pour la première fois, Trend Micro vous recommande de modifier votre mot de passe pour optimiser la sécurité de votre compte Hosted Email Security. (Voir *Administration* à la page 5-11.)

Utilisation de la console Web Hosted Email Security

La console Web Hosted Email Security aux administrateurs de messagerie de créer des rapports, visualiser des journaux, effectuer des tâches administratives et configurer ou modifier des stratégies.

Consultez les fichiers d'aide en ligne pour des informations détaillées sur l'utilisation de la console Web Hosted Email Security. Vous pouvez accéder à l'intégralité de l'aide en ligne en cliquant sur « Sommaire et Index » dans le menu déroulant Aide, ou accéder à un écran d'aide particulier en cliquant sur le point d'interrogation bleu ( ) dans le coin supérieur droit de chaque écran.

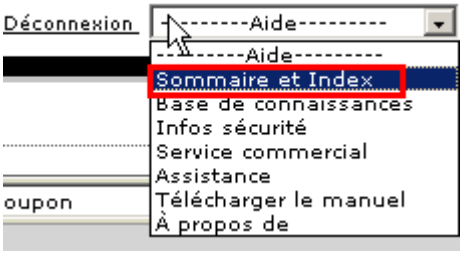


FIGURE 2-4. Menu déroulant d'aide

Rapports

L'écran Tableau de bord (*figure 2-5*) s'affiche lorsque vous vous connectez à Hosted Email Security. Le *Tableau 2-2* à la page 2-13 décrit les graphiques du tableau de bord.

Les utilisateurs de Hosted Email Security peuvent rechercher des messages entrants et sortants. Sélectionnez **Entrant** ou **Sortant** dans la liste déroulante « Direction du trafic de messages ».

Pour des données spécifiques sur les actions Hosted Email Security, cliquez sur l'onglet adéquat ou double-cliquez sur l'image de l'écran Tableau de bord.

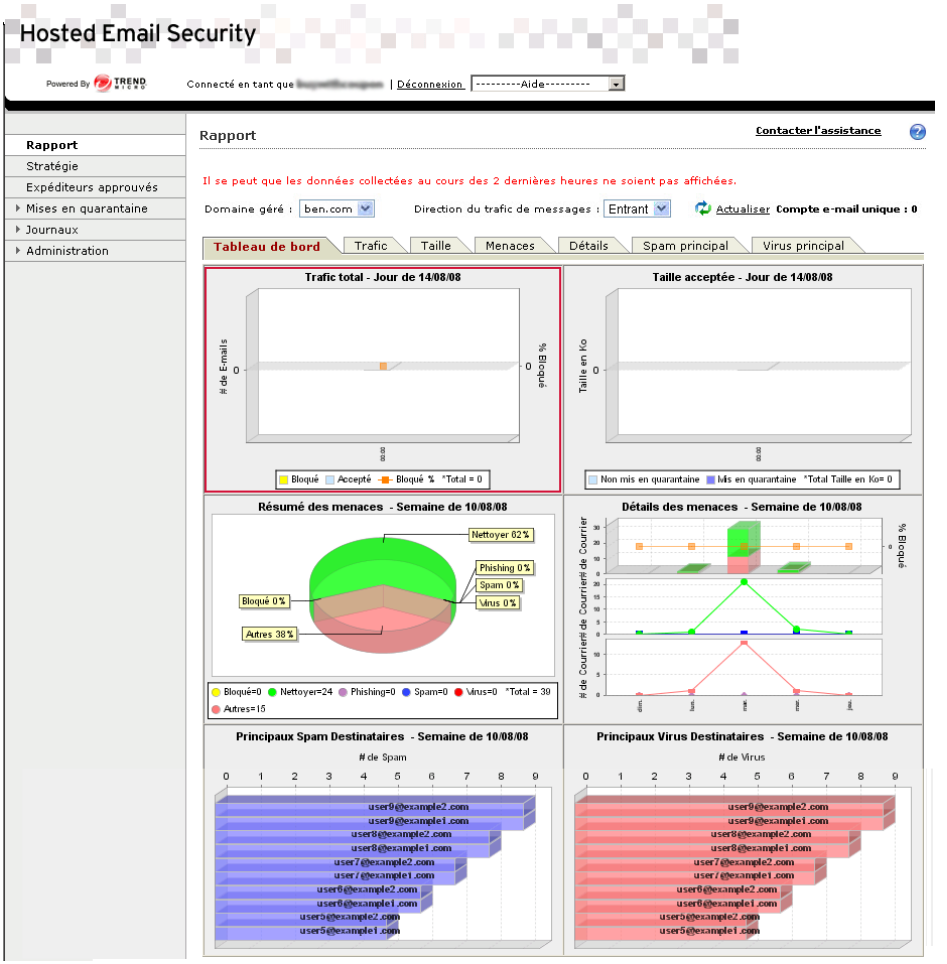


FIGURE 2-5. Écran Rapport de résumé (trafic entrant)

Tableau 2-2 à la page 2-13 décrit les graphiques de l'onglet Tableau de bord.

TABLEAU 2-2. Graphiques de l'écran Tableau de bord

NOM DU GRAPHIQUE	NOM DE L'ONGLET	DESCRIPTION
Trafic total	Trafic	Indique le trafic total de messages bloqués et acceptés pour le domaine sélectionné
Taille acceptée	Taille	Indique le volume total du trafic (en Ko) des messages acceptés pour le domaine sélectionné
Résumé des menaces	Menaces	Indique le pourcentage des types spécifiques de messages qui composent le trafic d'e-mails pour le domaine de messagerie sélectionné.
Détails des menaces	Détails	Indique la distribution détaillée du trafic de messages pour le domaine de messagerie sélectionné*
Principaux destinataires de spams Principaux expéditeurs de spams	Spam principal	Présente les principaux destinataires de spams (ou expéditeurs, pour les messages sortants) pour le domaine de messagerie sélectionné.
Principaux destinataires de virus Principaux expéditeurs de virus	Virus principal	Présente les principaux destinataires de virus (ou expéditeurs, pour les messages sortants) pour le domaine de messagerie sélectionné.

*. Pour éviter d'encombrer le tableau de bord, la légende de ce rapport en est exclue.

Onglet Trafic

Cliquez sur l'onglet **Trafic** pour afficher l'écran Trafic total (*figure 2-6*). Celui-ci indique le trafic total de messages bloqués et acceptés pour le domaine sélectionné à chaque intervalle de temps et la tendance du trafic pour la période sélectionnée. La légende indique le nombre de messages bloqués, de messages acceptés pour traitement postérieur, le pourcentage de trafic bloqué et le nombre total d'e-mails pour le domaine sélectionné. Pour une meilleure visibilité, le graphique « % bloqués » dispose de sa propre échelle, à droite du graphique.

Remarque : L'affichage du trafic « bloqué » a une signification différente selon qu'il s'agit de trafic entrant ou sortant. Le trafic entrant est filtré par les services de réputation de messagerie (Email Reputation Services ou ERS) de Trend Micro, ce qui n'est pas le cas du trafic sortant. Si les messages sont bloqués dans le trafic sortant, la raison du blocage n'est pas liée à la réputation de messagerie, mais peut être due à des problèmes avec le service de relais de messages Hosted Email Security, comme expliqué plus bas.

Pour les messages entrants :

- **Bloqués :** Nombre de tentatives d'envoi de messages malveillants vers le domaine sélectionné. Ce trafic de messages malveillants représente des connexions bloquées par le filtre Trend Micro Email Reputation Services (ERS).
- **Acceptés :** Nombre de messages ayant passé le filtre ERS et acceptés pour traitement ultérieur par Trend Micro Hosted Email Security.
- **% bloqués :** Pourcentage du trafic de messages bloqués par ERS pour le domaine de messagerie sélectionné.
- **Total :** Nombre total de messages traités par Hosted Email Security, pour le domaine de messagerie sélectionné. Il s'agit de la somme du trafic bloqué et accepté.

Pour les messages sortants uniquement :

- **Bloqué :** Nombre de tentatives de messages rejetées par le serveur relais de messages Hosted Email Security. Les raisons possibles du blocage sont les suivantes :
  - L'adresse du destinataire ne peut pas être résolue (« `personne@???.com` »).
  - Des spammeurs ont falsifié l'adresse de l'expéditeur afin que le message semble provenir du domaine du client.
  - Le serveur de messagerie du client est compromis (par un relais ouvert, par exemple) et envoie des messages de spam.

Remarque : Les messages sortants ne sont pas bloqués par le filtre ERS (Email Reputation Services) de Trend Micro mais par le service relais de messages Hosted Email Security.

- **Acceptés :** Nombre de messages acceptés par Trend Micro Hosted Email Security pour un traitement ultérieur.
- **% bloqués :** Pourcentage du trafic de messages bloqués par le service relais de messages Hosted Email Security, pour le domaine de messagerie sélectionné.
- **Total :** Nombre total de messages traités par Hosted Email Security, pour le domaine de messagerie sélectionné. Il s'agit de la somme du trafic bloqué et accepté.

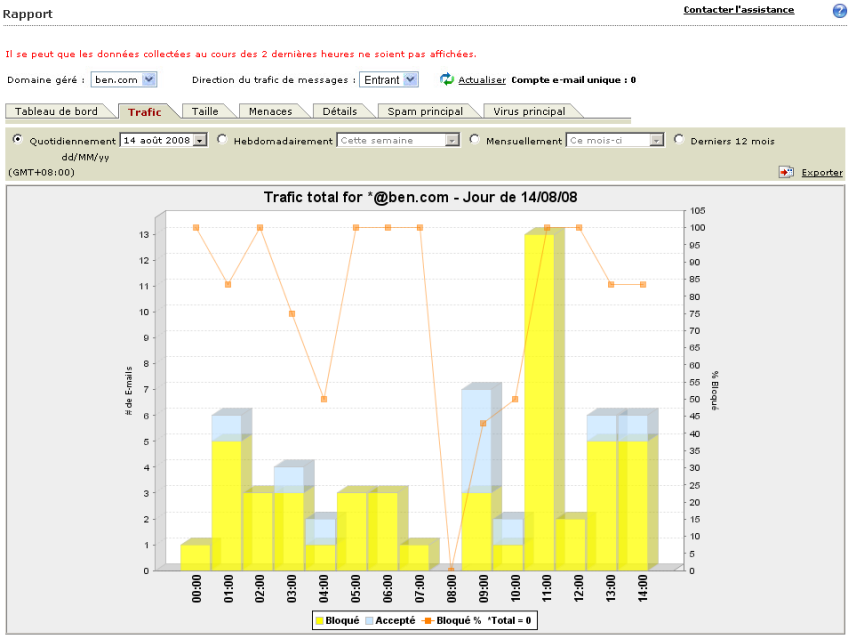


FIGURE 2-6. Écran Rapport de résumé (trafic entrant)

Onglet Taille

Cliquez sur l'onglet **Taille** pour afficher le rapport Taille acceptée (*figure 2-7*). Celui-ci indique le volume total du trafic (en Ko) des messages acceptés pour le domaine sélectionné. La période concernée par le rapport est, par défaut, *aujourd'hui* (ce jour). La légende indique la taille totale des messages non mis en quarantaine, des messages en quarantaine et la taille totale des messages acceptés. Cet onglet peut afficher un graphique du trafic entrant ou sortant, selon la direction du trafic de messages sélectionnée.

Non mis en quarantaine : taille des messages acceptés, qui n'ont pas été mis en quarantaine, pour le domaine de messagerie sélectionné.

Mis en quarantaine : taille des messages mis en quarantaine pour le domaine de messagerie sélectionné. Si la quarantaine n'est pas configurée dans les stratégies pour ce domaine de messagerie, il n'y aura aucun message mis en quarantaine représenté dans ce graphique.

Taille totale : nombre total de messages acceptés pour le domaine de messagerie sélectionné. Il s'agit de la somme des messages mis en quarantaine et non mis en quarantaine.

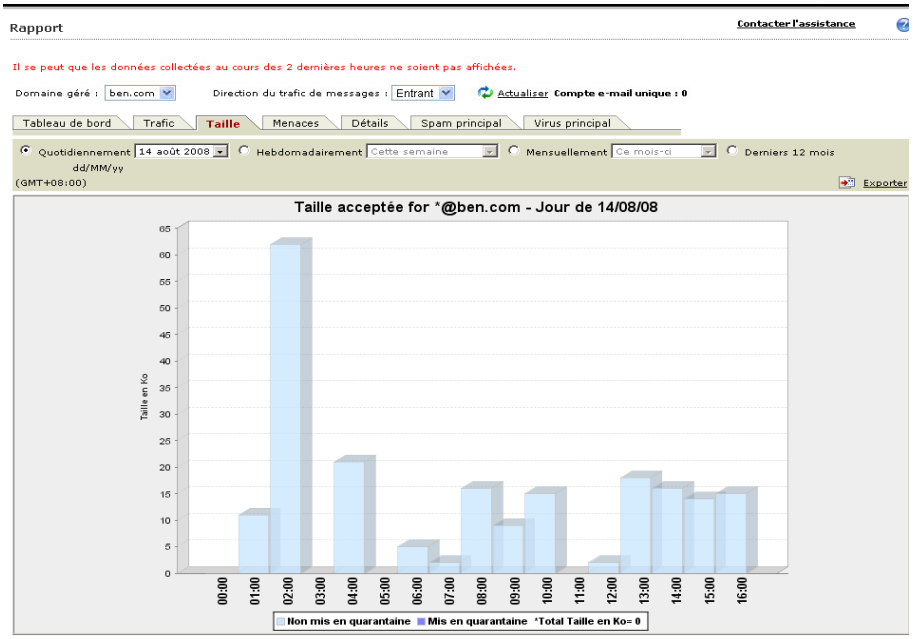


FIGURE 2-7. Écran Rapport Taille acceptée (trafic entrant)

Onglet Menaces

Cliquez sur l'onglet **Menaces** pour afficher le rapport de résumé sur les menaces (*figure 2-8*), lequel affiche la proportion de messages par type pour le domaine sélectionné. La période concernée par le rapport est, par défaut, la semaine en cours. Le graphique circulaire présente les pourcentages des différents types de messages du domaine sélectionné.

La légende indique le nombre de messages bloqués, les messages sains, les messages de phishing, les spams, les virus, ainsi que le nombre total de messages du domaine de messagerie sélectionné.

- **Bloqués** : Pour le domaine de messagerie sélectionné, nombre de connexions de messagerie bloquées par Trend Micro ERS (pour les messages entrants) ou par le service relais de messages Hosted Email Security (pour les messages sortants).
- **Sains** : Pour le domaine de messagerie sélectionné, nombre d'e-mails jugés « sains » par Hosted Email Security.
- **Phishing** : Nombre de messages identifiés par Hosted Email Security comme messages de phishing pour le domaine de messagerie sélectionné.
- **Spam** : Pour le domaine de messagerie sélectionné, nombre de messages identifiés comme spams par le moteur heuristique anti-spam de Hosted Email Security.
- **Virus** : Nombre d'e-mails identifiés par Hosted Email Security comme porteurs de virus pour le domaine de messagerie sélectionné.
- **Autres** : Nombre d'e-mails filtrés par d'autres filtres de contenu Hosted Email Security (tels que le filtre de taille de pièce jointe), pour le domaine de messagerie sélectionné.
- **Total** : Nombre total d'e-mails pour le domaine de messagerie sélectionné. Il s'agit de la somme des six catégories.

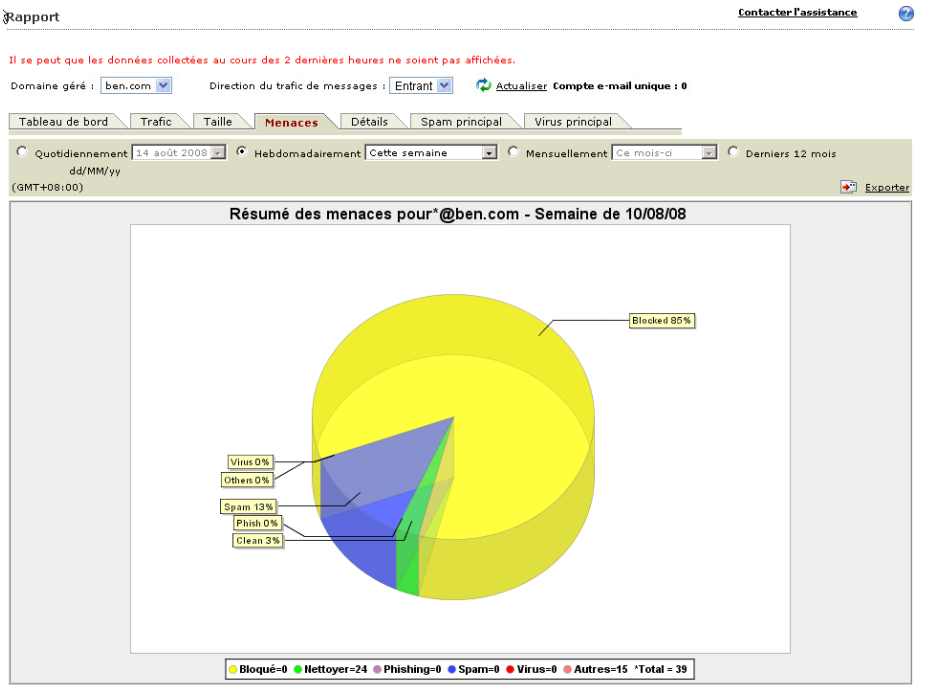


FIGURE 2-8. Écran Rapport de résumé des menaces (trafic entrant)

Onglet Détails

Cliquez sur l'onglet **Détails** pour afficher le Rapport de détail des menaces (*figure 2-13*). Celui-ci présente la distribution précise du trafic de messages pour le domaine de messagerie sélectionné. La période concernée par le rapport est, par défaut, la semaine en cours. Ce rapport utilise les mêmes couleurs que les autres. Il présente trois graphiques détaillés et un tableau de totaux :

Graphique 1 : nombre de messages et pourcentage de trafic bloqué, comme illustré dans la *figure 2-9*.

Remarque : L'affichage du trafic « bloqué » a une signification différente selon qu'il s'agit de trafic entrant ou sortant, comme expliqué en détails dans la section *Onglet Trafic* à partir de la page 2-13.

Ce graphique est similaire au rapport sur le Trafic total présenté plus haut. Il classe de manière plus précise les messages acceptés en diverses catégories comme les virus, le phishing, les spams, les messages sains, etc.

- L'axe vertical sur la gauche correspond aux barres verticales indiquant le nombre total de messages pour le domaine de messagerie sélectionné. Chaque barre verticale représente le nombre de messages bloqués, sains, de phishing, de spams, de virus, etc.
- L'axe vertical sur la droite correspond au graphique de lignes qui représente le pourcentage de tout le trafic bloqué par le service ERS (Trend Micro Email Reputation Service) pour chaque intervalle de temps.

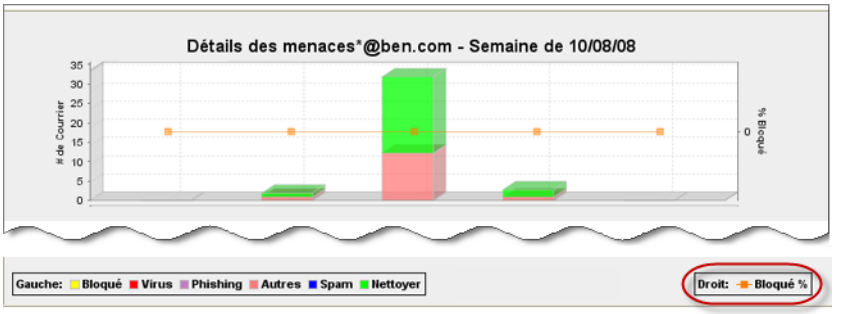


FIGURE 2-9. Rapport de détail des menaces, graphique 1 (trafic entrant)

Graphique 2 : nombre de messages de chaque catégorie « spams » et « sains » uniquement

Chaque ligne représente le nombre de messages d'un certain type à chaque intervalle, comme illustré dans la *figure 2-10*.

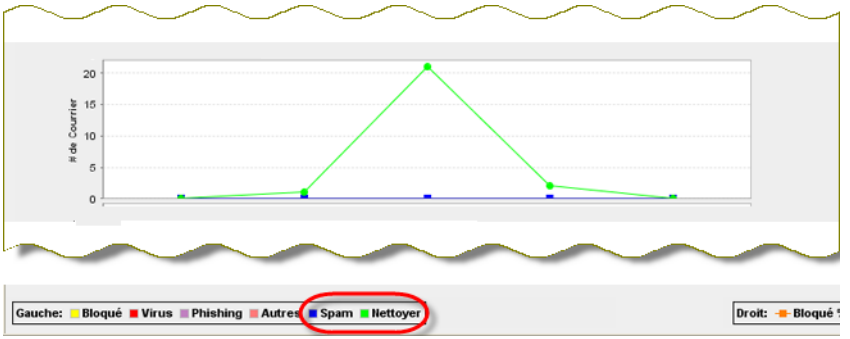


FIGURE 2-10. Rapport de détail des menaces, graphique 2 (trafic entrant)

Graphique 3 : nombre de messages de chaque catégorie : « virus », « phishing » et « autres » uniquement

Chaque ligne représente le nombre de menaces de messages d'un certain type à chaque intervalle., comme illustré dans la *figure 2-11*.

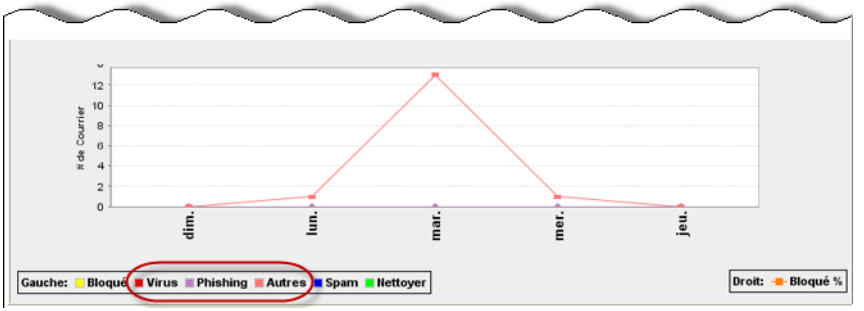
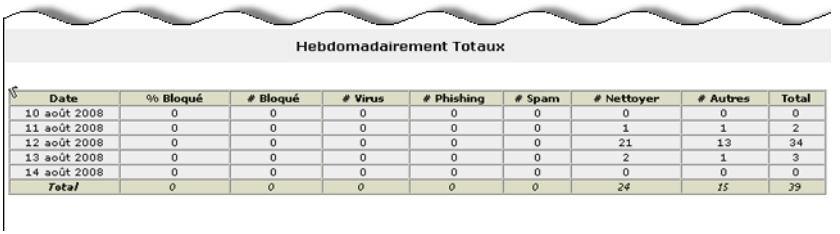


FIGURE 2-11. Rapport de détail des menaces, graphique 3

Tableau des totaux : propose une compilation hebdomadaire des totaux pour les critères suivants :

- Pourcentage de messages bloqués
- Nombre de messages bloqués
- Nombre de virus
- Nombre de phishing
- Nombre de spams
- Nombre de messages nettoyés
- Autres
- Total quotidien

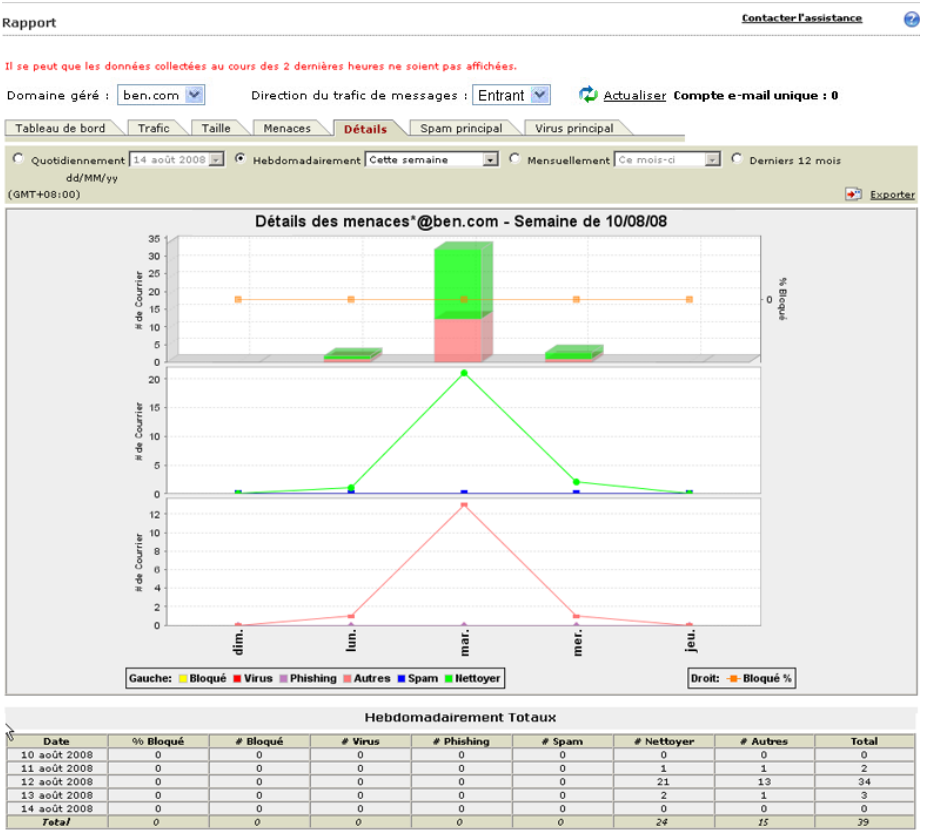


Hebdomadairement Totaux

Date	% Bloqué	# Bloqué	# Virus	# Phishing	# Spam	# Nettoyer	# Autres	Total
10 août 2008	0	0	0	0	0	0	0	0
11 août 2008	0	0	0	0	0	1	1	2
12 août 2008	0	0	0	0	0	21	13	34
13 août 2008	0	0	0	0	0	2	1	3
14 août 2008	0	0	0	0	0	0	0	0
Total	*0*	*0*	*0*	*0*	*0*	*24*	*15*	*39*

FIGURE 2-12. Rapport de détail des menaces, tableau des totaux

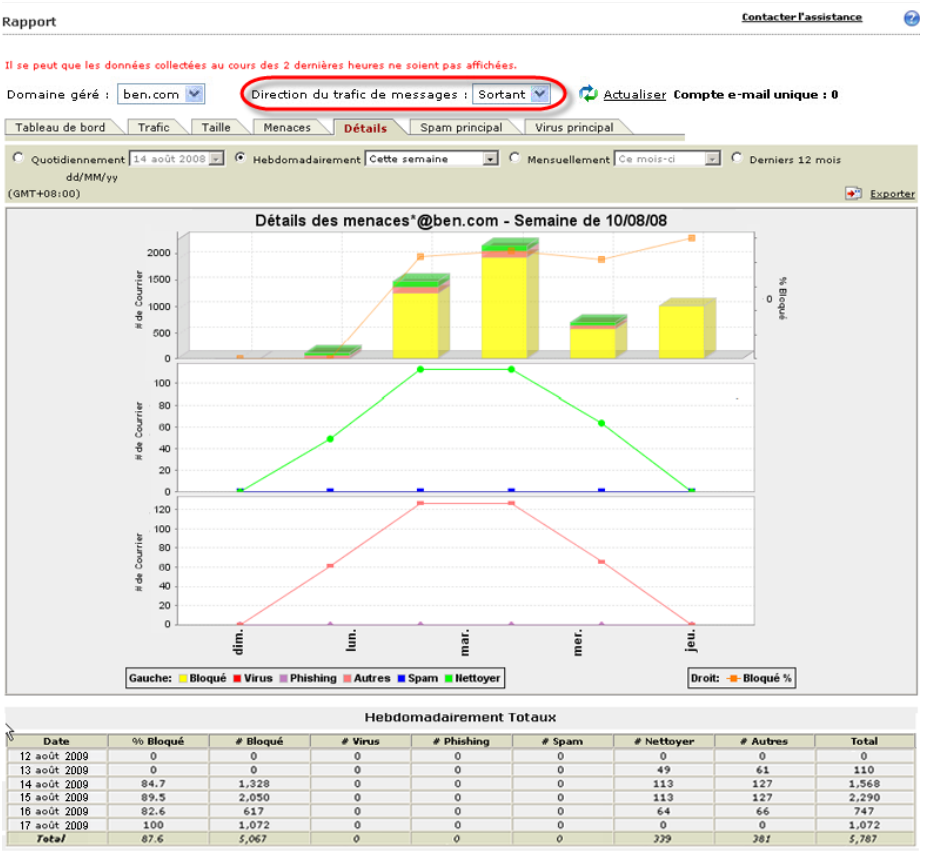
Remarque : Pour éviter d'encombrer le tableau de bord, la légende de ce rapport en est exclue.



Hebdomadairement Totaux

Date	% Bloqué	# Bloqué	# Virus	# Phishing	# Spam	# Nettoyer	# Autres	Total
10 août 2008	0	0	0	0	0	0	0	0
11 août 2008	0	0	0	0	0	1	1	2
12 août 2008	0	0	0	0	0	21	13	34
13 août 2008	0	0	0	0	0	2	1	3
14 août 2008	0	0	0	0	0	0	0	0
Total	*0*	*0*	*0*	*0*	*0*	*24*	*15*	*39*

FIGURE 2-13. Écran Rapport de détail des menaces (trafic entrant)



Hebdomadairement Totaux

Date	% Bloqué	# Bloqué	# Virus	# Phishing	# Spam	# Nettoyer	# Autres	Total
12 août 2009	0	0	0	0	0	0	0	0
13 août 2009	0	0	0	0	0	49	61	110
14 août 2009	84.7	1,328	0	0	0	113	127	1,568
15 août 2009	89.5	2,050	0	0	0	113	127	2,290
16 août 2009	82.6	617	0	0	0	64	66	747
17 août 2009	100	1,072	0	0	0	0	0	1,072
Total	*87.6*	*5,067*	*0*	*0*	*0*	*339*	*381*	*5,787*

FIGURE 2-14. Écran Rapport de détail des menaces (trafic sortant)

Onglet Spam principal

Cliquez sur l'onglet **Spam principal** pour afficher le rapport des principaux destinataires de spams (*figure 2-15*) ou principaux expéditeurs de spams. Selon la direction du trafic de messages choisie, celui-ci présente les principaux destinataires ou expéditeurs de spams pour le domaine de messagerie sélectionné. La période de rapport par défaut est *cette semaine*. Les rapports sur les principaux destinataires de spams sont affichés à l'heure GMT.

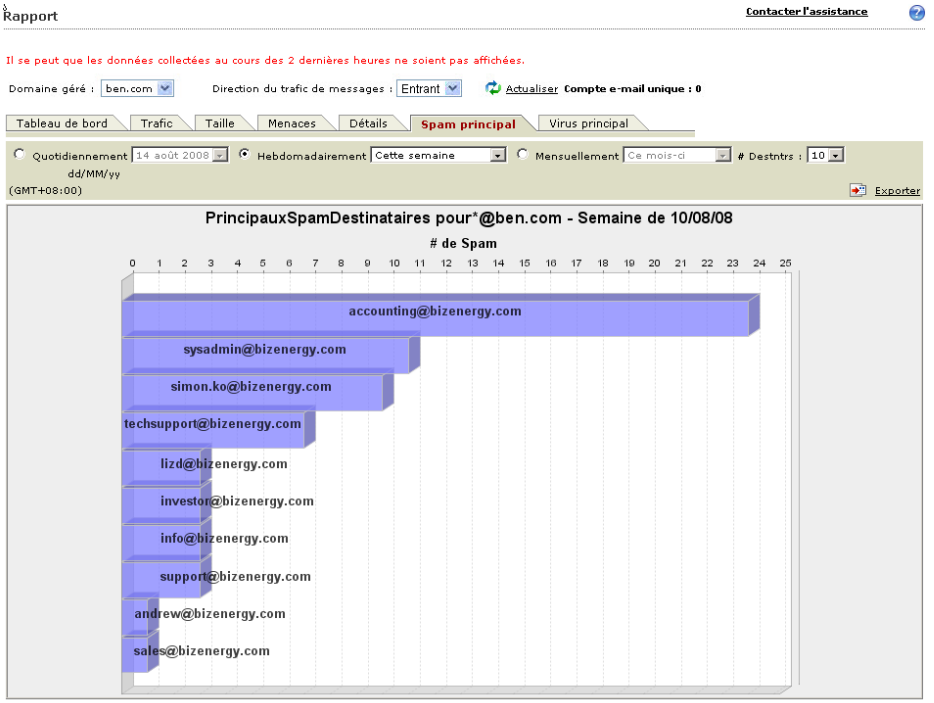


FIGURE 2-15. Écran Rapport des principaux destinataires de spams (trafic entrant)

Onglet Virus principaux

Cliquez sur l'onglet **Virus principaux** pour afficher les principaux destinataires de virus (*figure 2-16*) ou le rapport des principaux expéditeurs de virus pour le domaine de messagerie sélectionné. Sélectionnez « entrant » dans la liste déroulante de la direction du trafic de messages pour afficher le rapport des destinataires ou « sortant » pour le rapport des expéditeurs. La période concernée par le rapport est, par défaut, la *semaine en cours*. Les rapports sur les principaux destinataires/expéditeurs de virus sont affichés à l'heure GMT.

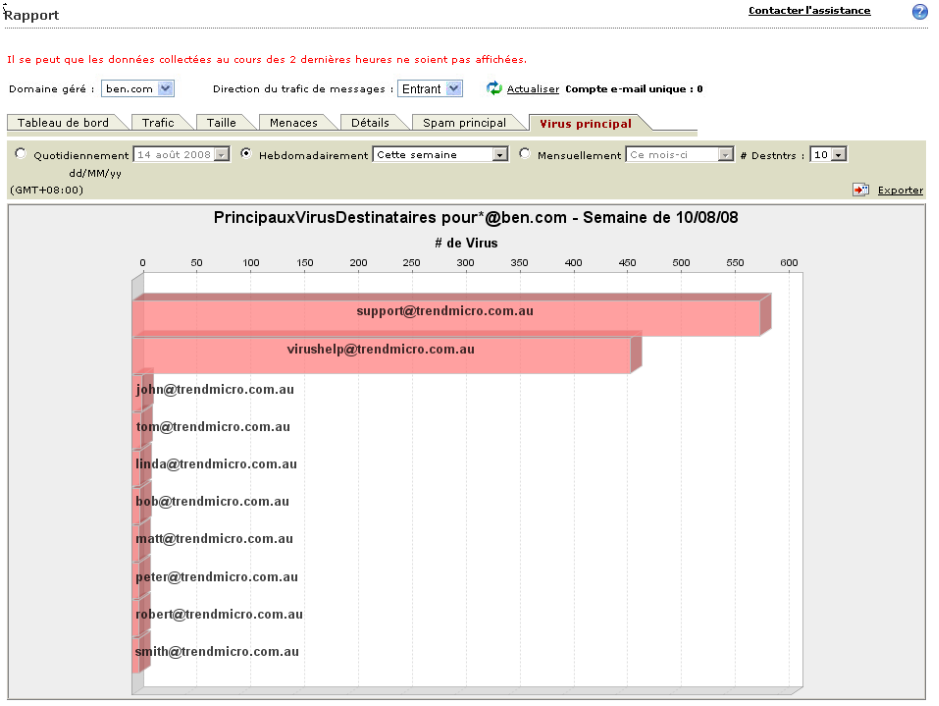


FIGURE 2-16. Écran Rapport des principaux destinataires de virus (trafic entrant)

Chapitre 3

Gestion des stratégies

Ce chapitre indique comment créer et gérer des stratégies de scan à l'aide de la console d'administration Hosted Email Security.

Sujets abordés dans ce chapitre :

- *Vue d'ensemble des stratégies* à la page 3-2
- *Paramètres de stratégie par défaut* à la page 3-3
- *Filtrage de contenu* à la page 3-6
- *Actions de règle* à la page 3-13
- *Ordre d'exécution des règles* à la page 3-26
- *Ajout et modification de règles* à la page 3-28

Vue d'ensemble des stratégies

Une stratégie Hosted Email Security est définie par un ensemble de règles pour un domaine de messagerie spécifique. De multiples règles peuvent exister pour chaque domaine (stratégie), mais une seule stratégie existe par domaine.

À tout moment, les administrateurs peuvent consulter les règles qui s'appliquent à leur entreprise.

En fonction de votre niveau de service, vous pouvez afficher, modifier et créer des règles pour une stratégie de domaine spécifique.

Les clients de la **Version complète** disposent de droits de création et de modification.

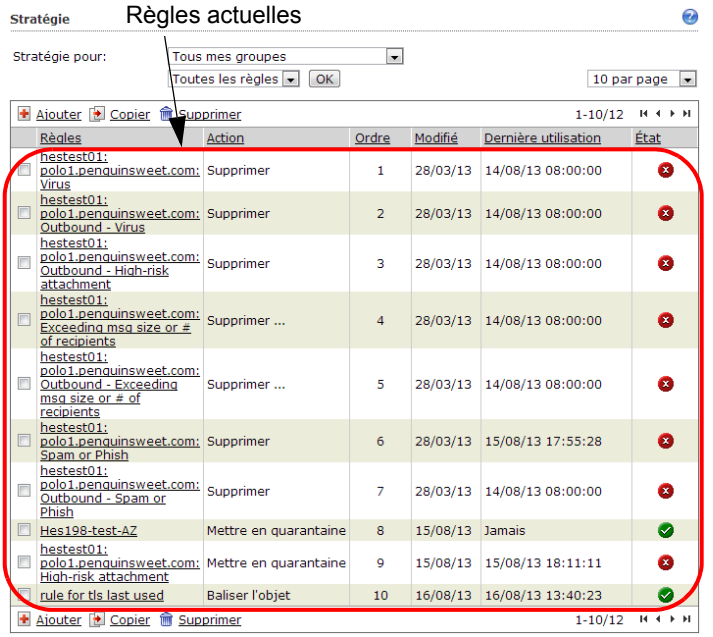


FIGURE 3-1. Écran Stratégie, version complète

L'écran Stratégie présente une liste des règles actuellement définies et l'état de chacune d'entre elles. Si vous disposez du niveau de service qui vous le permet, vous pouvez ajouter une nouvelle règle et modifier, copier ou supprimer des règles existantes à partir de cet écran. Pour obtenir une description des règles par défaut, consultez la section *Paramètres de stratégie par défaut* à la page 3-3.

En haut à droite de la liste des règles figurent le nombre de règles affichées sur cette page et le nombre total de règles. Vous pouvez filtrer la liste à l'aide des listes déroulantes situées en haut de l'écran.

Les règles sont affichées dans un tableau et triées dans l'ordre dans lequel elles sont appliquées pendant le scan effectué par Hosted Email Security. Le contenu de chaque tableau peut être réorganisé en cliquant sur l'en-tête de la colonne. Par exemple, cliquez sur l'en-tête de la colonne Action pour réorganiser le tableau dans l'ordre alphabétique par action. Cliquez sur la colonne Horodatage pour filtrer les règles en fonction de leur dernière date de modification. Sinon, cliquez sur Dernière utilisation pour afficher les règles en fonction de leurs dernières date et heure d'utilisation. Si la règle n'a pas été déclenchée, la valeur de la colonne est *Jamais*.

TABLEAU 3-1. Icônes activées et désactivées

ICÔNE	DESCRIPTION
	La règle est activée.
	La règle est désactivée.

Cliquez sur l'icône située à droite de chaque règle pour l'activer ou la désactiver.

Remarque : La désactivation d'une règle peut avoir des effets néfastes sur la sécurité de votre messagerie. Par exemple, la désactivation d'une règle de virus vous expose à des attaques de virus.

Paramètres de stratégie par défaut

Les règles suivantes font partie de la stratégie par défaut pour tous les clients Hosted Email Security.

Les clients de Hosted Email Security peuvent modifier les règles par défaut, ainsi que créer de nouvelles règles.

Règle 1 : Virus

Si l'un des éléments suivants est trouvé, le message est supprimé dans son intégralité.

a. Comportement d'envoi en masse : Conçu pour protéger l'utilisateur contre les virus qui sont souvent propagés par le biais d'envois en masse. Un message est identifié comme contenant un virus qui ne peut pas être nettoyé et il a un comportement d'envoi en masse.

b. Virus – non nettoyable : le message est identifié comme contenant un virus qui ne peut pas être nettoyé.

c. Virus – nettoyable : le message est identifié comme contenant un virus qui peut être nettoyé.

Règle 2 : Dépassement de la taille du message ou du nombre autorisé de destinataires

Cette règle est conçue pour protéger le système contre les attaques par refus de service (Denial of Service, DOS) ou de type « Zip of Death ». Si la taille du message entrant dépasse la limite par défaut de 50 Mo ou si celui-ci a été envoyé à plus de 50 destinataires, il est supprimé et Hosted Email Security en notifie l'expéditeur. Les clients Hosted Email Security peuvent modifier cette règle jusqu'à la limite proposée par le système de 100 destinataires.

Règle 3 : Spam ou phishing

Cette règle est conçue pour intercepter les e-mails de spam ou de phishing. L'action par défaut est de supprimer tous les messages identifiés comme des e-mails de spam ou de phishing. Tous les clients Hosted Email Security ont la possibilité de modifier l'action par défaut. Nous recommandons vivement de n'utiliser que les actions Supprimer ou Mettre en quarantaine pour cette règle. Tous les e-mails mis en quarantaine sont conservés dans la quarantaine Hosted Email Security accessible sur le Web pendant 21 jours dans la région EMEA et pendant 15 jours dans toutes les autres régions.

Les clients de Hosted Email Security peuvent modifier le critère utilisé pour le taux d'interception des spams entre Le plus bas (le moins agressif) et Le plus élevé (le plus agressif). Le paramètre par défaut est Modérément bas.

Remarque : Il existe deux règles par défaut en matière de spam. Pour les bulletins d'information ou les messages semblables aux spams, veuillez vous reporter à la règle *Règle 5 : Bulletin d'information ou message semblable au spam*.

Règle 4 : Pièce jointe à haut risque

Cette règle n'est disponible que pour les clients de Hosted Email Security. Elle supprime des e-mails les pièces jointes à haut risque telles que définies dans les critères de règle. Les exemples de pièces jointes à haut risque sont des fichiers exécutables à l'extension .exe ou des fichiers à contenu multimédia (.mp3) qui doivent être renommés en tant que fichier_inoffensif.txt. Si un message est identifié comme contenant une pièce jointe à haut risque, celle-ci est supprimée avant que l'e-mail ne soit transmis.

Règle 5 : Bulletin d'information ou message semblable au spam

Cette règle est conçue pour intercepter les « graymail » comme les bulletins d'information. L'action par défaut pour ces messages électroniques similaires aux spams est de « Baliser l'objet » (avec l'intitulé « Spam> »). Nous recommandons vivement de n'utiliser que les actions Baliser l'objet ou Mettre en quarantaine pour cette règle. Tous les e-mails mis en quarantaine sont conservés dans la quarantaine Hosted Email Security accessible sur le Web pendant 21 jours dans la région EMEA et pendant 15 jours dans toutes les autres régions.

Les clients de Hosted Email Security peuvent modifier le critère utilisé pour le taux d'interception des spams entre Le plus bas (le moins agressif) et Le plus élevé (le plus agressif). Le paramètre par défaut est Modérément élevé.

Remarque : Il existe deux règles par défaut en matière de spam. Pour les messages très semblables aux spams ou aux techniques de phishing, veuillez vous reporter à la règle *Règle 3 : Spam ou phishing*.

Règle 6 : Pièces jointes compressées protégées par mot de passe

Cette règle est conçue pour permettre aux utilisateurs de la version complète de configurer l'action destinée à gérer les messages électroniques contenant des pièces jointes compressées et protégées par mot de passe. Par défaut, les messages contenant des pièces jointes compressées protégées par mot de passe sont transmis au destinataire et un avertissement est ajouté dans le corps du message pour signaler que les pièces jointes n'ont pas été scannées.

Stratégies de filtrage sortant par défaut

Pour tous les utilisateurs Hosted Email Security, quatre règles par défaut supplémentaires seront ajoutées. Ces règles sont conçues à l'instar de leur équivalent ci-dessus, mais elles ne s'appliquent qu'aux messages sortants. Les règles par défaut pour le filtrage sortant sont les suivantes :

- Règle sortante - Virus
- Règle sortante - Pièce jointe à haut risque
- Règle sortante - Dépassement de la taille du message ou du nombre autorisé de destinataires
- Règle sortante - Spam ou phishing

Filtrage de contenu

Les utilisateurs de Hosted Email Security peuvent définir des règles de filtrage de contenu pour les e-mails. Hosted Email Security offre des options polyvalentes en termes de filtrage de contenu. Elles vous permettent d'identifier presque tout type de contenu.

Filtrage de contenu par mot-clé

Vous pouvez configurer les règles Hosted Email Security de manière à ce qu'elles comparent le contenu dans le cadre de leur logique d'exploitation. Hosted Email Security peut comparer le contenu grâce aux mots-clés, à des expressions récurrentes ou les deux. Configurez le filtrage de contenu à la deuxième étape lorsque vous ajoutez une nouvelle règle ou modifiez une règle existante.

Pour configurer le filtrage de contenu à l'aide des mots-clés :

1. Lors de l'ajout ou de la modification d'une règle, à l'étape 2 : Sélectionner les critères de scan, cliquez sur **Avancé.** Plusieurs possibilités s'affichent sous Avancé comme le montre la *figure 3-2* ci-dessous.

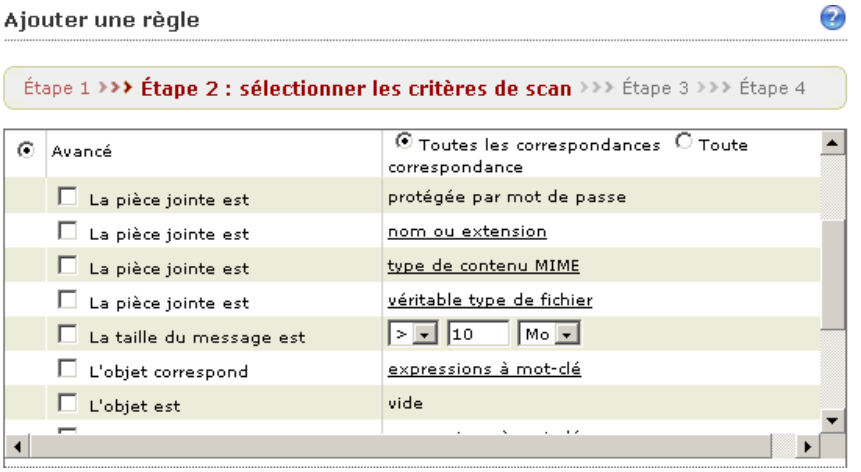


FIGURE 3-2. Options de filtrage du contenu

2. Sélectionnez la partie du message à analyser. Les choix suivants sont possibles :
   - Objet
   - Corps
   - En-tête spécifié
   - Pièce jointe
3. Cliquez sur le lien **expressions à mot-clé** à droite de votre sélection. L'écran Expressions à mot-clé s'affiche, comme l'indique la *figure 3-3* ci-dessous.

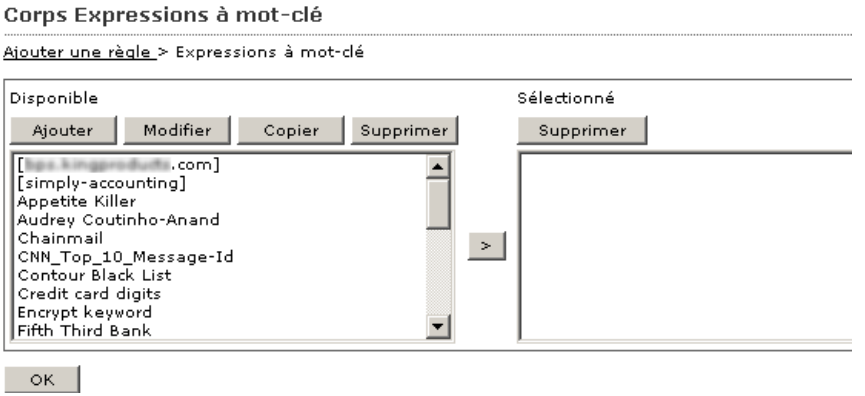


FIGURE 3-3. Ecran Expressions à mot-clé

4. Sélectionnez une ou plusieurs expressions existantes et cliquez sur la flèche Droite (>). Les expressions sélectionnées apparaissent dans la liste des éléments choisis dans la partie droite.
5. Vous pouvez éventuellement cliquer sur **Ajouter** pour créer une nouvelle expression, sur **Modifier** pour modifier une expression existante, sur **Copier** pour créer une copie et la modifier ou sur **Supprimer**.
6. Cliquez sur **Terminé**. Hosted Email Security enregistre vos sélections et réaffiche l'étape 2 principale : Sélectionner les critères de scan.
7. Répétez les étapes suivantes pour chaque partie du message dont vous souhaitez filtrer le contenu.
8. Lorsque vous avez terminé d'ajouter les critères de filtrage avancés, sélectionnez **Toutes les correspondances** (valeur par défaut) ou **Toute correspondance** dans la colonne à droite de l'option « Avancé » pour définir si l'e-mail doit répondre à tous les critères sélectionnés ou à l'un d'entre eux seulement pour activer la règle.
9. Cliquez sur **Suivant** et terminez la règle conformément aux instructions de la rubrique *Ajout d'une nouvelle règle* à la page 3-28.

Filtrage de contenu à l'aide des expressions régulières

Pour configurer le filtrage de contenu à l'aide d'expressions régulières :

1. Suivez l'*Étape 1* à l'*Étape 3* ci-dessus pour afficher l'écran Expressions à mot-clé.
2. Cliquez sur **Ajouter** pour créer une nouvelle expression, ou sélectionnez une expression existante et cliquez sur **Modifier.** L'écran Expressions à mot-clé s'affiche dans un nouveau format, comme l'indique la *figure 3-4* ci-dessous.

FIGURE 3-4. Écran Expressions à mot-clé pour expressions régulières

3. Dans le champ **Nom de liste**, entrez un nom pour l'expression si vous en créez une nouvelle. (Si vous modifiez une expression, le nom existant figure dans le champ.)
4. Dans la liste déroulante **Correspondance**, sélectionnez l'une des valeurs suivantes :
   - **N'importe lequel spécifié** – Toutes les correspondances pour les mots clés ou expressions régulières dans la liste.
   - **Tous spécifiés** – La valeur doit correspondre à tous les mots-clés et/ou expressions régulières dans la liste afin d'être considérée comme une correspondance.
   - **Pas les spécifiés** – Équivaut à l'opérateur .NOT. La correspondance est obtenue si le contenu ne correspond à aucun des mots-clés ou expressions régulières figurant dans la liste.

- **Uniquement lorsque le score combiné dépasse le seuil** – En cas de sélection, cette option affiche le champ « Score total de messages pour déclencher une action ». Avec cette option, les filtres Hosted Email Security filtrent le contenu à la recherche des expressions figurant dans la liste uniquement si le total des spams dépasse la limite définie (la valeur par défaut est 2).

5. Cliquez sur **Ajouter**. L'écran Ajouter des expressions à mot-clé apparaît alors.
6. Dans la zone de texte, tapez n'importe quelle combinaison de mots-clés et d'expressions régulières pour définir une expression à mot-clé (sans saut de ligne). Les opérateurs disponibles pour les expressions régulières sont indiqués ci-dessous :

   \ | ( ) { } [ ] . ^ $ * + ?

Conseil : Pour utiliser un opérateur comme expression littérale, vous devez le faire précéder d'une barre oblique inversée (\). Trend Micro conseille l'utilisation d'expressions régulières uniquement si vous disposez des connaissances requises. Hosted Email Security n'accepte pas les expressions ne respectant pas la syntaxe appropriée en vigueur.

7. Cliquez sur **Enregistrer.** L'écran Expressions régulières comprend un tableau contenant les expressions que vous avez créées comme l'indique la *figure 3-5* ci-dessous.

FIGURE 3-5. Les expressions à mot-clé ont été ajoutées.

8. Cochez la case **Sensible à la casse** si nécessaire. Si vous avez sélectionné **Uniquement lorsque le score combiné dépasse le seuil** pour le champ Correspondance et que vous avez ajouté plusieurs expressions, sélectionnez la pondération pour chaque expression comme l'indique la rubrique *Pondération des listes d'expressions à mot-clé* à la page 3-12.
9. Cliquez sur **Enregistrer**. La liste des expressions que vous venez de créer s'affiche dans la liste « Disponible » dans la zone située à gauche comme l'indique la *figure 3-6* ci-dessous.

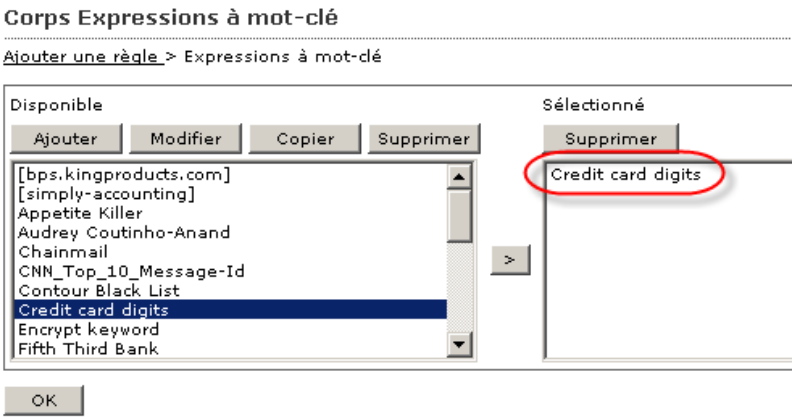


FIGURE 3-6. Ajout d'une expression à mot-clé à une règle

10. Pour ajouter un nouveau critère à une règle, sélectionnez le nom dans la liste située à gauche, cliquez sur la flèche Droite (>) et ensuite sur **Terminé**. Hosted Email Security ajoute les critères à la règle que vous créez.
11. Cliquez sur **Suivant** et terminez la règle conformément aux instructions de la rubrique *Ajout d'une nouvelle règle* à la page 3-28.

Pondération des listes d'expressions à mot-clé

Lorsque vous créez une liste d'expressions à mot-clé, vous pouvez affecter une pondération à chaque expression de la liste.

Si la liste déroulante Correspondance est réglée sur « Uniquement lorsque le score combiné dépasse le seuil », vous devez définir un score global pour l'expression régulière ainsi qu'un score individuel pour chaque composant.

Pour utiliser la pondération sur les listes d'expressions à mot-clé :

1. Vérifiez si vous avez bien sélectionné **Uniquement lorsque le score combiné dépasse le seuil** dans la liste déroulante Correspondance.
2. Tapez une pondération totale dans le champ **Score total de messages pour déclencher**.
3. Dans la colonne **Score**, sélectionnez une pondération pour chaque expression de la liste comme l'indique la *figure 3-7* ci-dessous.

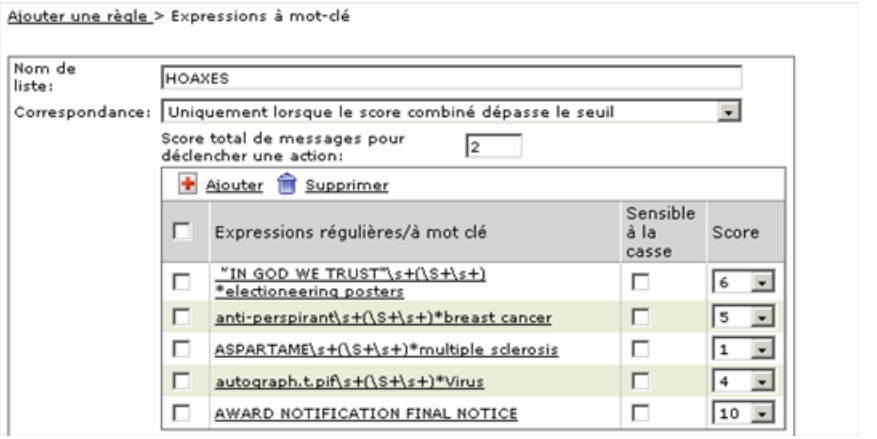


FIGURE 3-7. Pondération des expressions à mot-clé

4. Cochez éventuellement la case **Sensible à la casse**.
5. Cliquez sur **Enregistrer**.

Pour chaque expression à mot-clé correspondant au contenu d'un e-mail, Hosted Email Security augmentera le score des mots-clés du message en fonction du nombre défini dans la colonne Score. Par exemple, si deux mots d'un message correspondent à des mots clés d'une liste nommée « Blasphème », avec un score de 2, le score de ce message sera de 4.

Si le score total dépasse le nombre défini dans le champ « Score total de messages pour déclencher », la règle est déclenchée. Par exemple, si deux correspondances de listes de mots-clés sont déclenchées pour un score de message de 4 et que la valeur du champ Score total de messages pour déclencher est de 3, la règle est déclenchée.

Actions de règle

Hosted Email Security fournit un nombre d'actions que vous pouvez utiliser lorsque vous élaborez ou modifiez une règle. Les actions accessibles aux utilisateurs de Hosted Email Security sont les suivantes :

- *Supprimer le message entier* à la page 3-13
- *Envoyer le message maintenant* à la page 3-14
- *Mettre le message en quarantaine* à la page 3-15
- *Nettoyer les virus nettoyables et supprimer ceux qui ne peuvent pas être nettoyés* à la page 3-16
- *Supprimer les pièces jointes correspondantes* à la page 3-16
- *Insérer un horodatage dans le corps du message* à la page 3-17
- *Baliser la ligne d'objet* à la page 3-17
- *Envoyer un message de notification* à la page 3-18
- *Copier en copie cachée (BCC) un autre destinataire* à la page 3-19
- *Rejeter le message* à la page 3-20
- *Contourner une règle* à la page 3-20
- *Chiffrer des e-mails* à la page 3-21 (disponible séparément)

Ces actions sont exécutées dans un ordre prédéfini basé sur la logique de traitement intégrée à Hosted Email Security. Pour plus d'informations sur l'ordre d'exécution, consultez la rubrique *Ordre d'exécution des règles* à la page 3-26.

Supprimer le message entier

Cette action supprime le message et toutes ses pièces jointes. Le message est enregistré comme ayant été supprimé dans les journaux Hosted Email Security, mais une fois qu'il est supprimé, le message ne peut pas être récupéré. Elle entre dans la catégorie des actions de type Intercepter (voir *Actions Intercepter* à la page 3-26).

Pour configurer une action de règle afin de supprimer un message :

1. Sélectionnez l'action **Supprimer le message entier** à partir de la section Intercepter.
2. Cliquez sur **Suivant** si vous créez une nouvelle règle ou sur **Enregistrer** si vous modifiez une règle existante.

Envoyer le message maintenant

Utilisez l'action Envoyer maintenant pour envoyer immédiatement un e-mail. Lorsque cette action prend effet, Hosted Email Security envoie l'e-mail sans exécuter davantage de règles pour l'e-mail concerné.

Toutes les règles sont organisées automatiquement pour des raisons de sécurité et d'efficacité d'exécution. Les administrateurs n'ont pas à déterminer l'ordre d'exécution des règles. L'action Envoyer maintenant contourne l'ordre automatique d'exécution, de sorte que Hosted Email Security peut envoyer l'e-mail immédiatement.

AVERTISSEMENT ! L'action « Envoyer maintenant » n'est pas recommandée comme action unique. Si vous choisissez « Envoyer maintenant » en tant qu'action unique pour les messages de spam, par exemple, tous ces messages seront simplement envoyés à vos destinataires, comme si aucun filtre anti-spam n'était en place.

Si vous utilisez « Envoyer maintenant » avec une règle de virus, vérifiez que vous avez également configuré une action « Supprimer » pour la règle de virus. Seule l'action « Supprimer » dispose d'un degré de priorité supérieur à l'action « Envoyer maintenant », et elle sera donc traitée avant cette dernière (puis mettra fin au traitement de cette règle).

Pour configurer une action de règle afin d'envoyer un message immédiatement:

1. Sélectionnez l'action **Envoyer maintenant** dans la section Intercepter.
2. Cliquez sur **Suivant** si vous créez une nouvelle règle ou sur **Enregistrer** si vous modifiez une règle existante.
3. Cliquez sur **OK** sur le message Envoyer maintenant qui s'affiche. Le message se ferme.

4. Si vous créez une nouvelle règle, tapez un nom de règle dans le champ **Nom de la règle**.
5. Cliquez sur **Enregistrer**.

AVERTISSEMENT ! Si vous choisissez « Envoyer maintenant » en tant qu'action unique pour une règle de virus, les e-mails contenant des virus pourraient s'infiltrer sans être bloqués.

Mettre le message en quarantaine

Si votre niveau de service comprend l'action Mettre en quarantaine, celle-ci place le message et toutes les pièces jointes dans la zone de quarantaine configurée dans la règle. Elle entre dans la catégorie des actions de type Intercepter (voir la rubrique *Actions Intercepter* à la page 3-26).

Pour configurer une action de règle afin de mettre un message en quarantaine :

1. À partir de la section Intercepter de l'écran Actions de règles, sélectionnez l'action **Mettre en quarantaine**.
2. Sélectionnez une zone de quarantaine dans la liste déroulante, ou cliquez sur **Modifier** pour créer une nouvelle zone de quarantaine.

Remarque : Les éléments mis en quarantaine sont maintenant stockés dans une structure de répertoire créée par Hosted Email Security. Cela permet d'améliorer la performance lorsque le produit enregistre les éléments dans les quarantaines ou lorsque les utilisateurs les affichent par le biais d'une console Web. Les messages mis en quarantaine sont indexés dans la base de données Hosted Email Security pour que vous puissiez utiliser des requêtes et des outils de recherche améliorés.

---

3. Cliquez sur **Suivant** si vous créez une nouvelle règle ou sur **Enregistrer** si vous modifiez une règle existante.

Nettoyer les virus nettoyables et supprimer ceux qui ne peuvent pas être nettoyés

Cette action nettoie les virus nettoyables (ou autres menaces configurées) contenus dans les pièces jointes aux messages électroniques. Si la menace ne peut pas être nettoyée, la pièce jointe au message sera supprimée. Le nettoyage des virus nettoyables entre dans la catégorie des actions de type Modifier (voir la rubrique *Actions Modifier* à la page 3-27).

Remarque : L'action « Nettoyer les virus nettoyables » n'est disponible que lorsque le critère Virus est sélectionné dans la définition de règle. Par exemple :

Si cette action est utilisée dans la règle et que le message contient un virus impossible à nettoyer, le message sera supprimé.

Si les actions « Supprimer les pièces jointes correspondantes » et « Nettoyer les virus nettoyables » sont toutes deux utilisées dans la même règle, une pièce jointe contrevenante sera directement supprimée et l'action « Nettoyer les virus nettoyables » ne sera pas appliquée.

Pour configurer une action de règle pour nettoyer les pièces jointes infectées par des virus :

1. À partir de la section Modifier de l'écran Action, sélectionnez l'action **Nettoyer les fichiers infectés par un virus**.
2. Cliquez sur **Suivant** si vous créez une nouvelle règle ou sur **Enregistrer** si vous modifiez une règle existante.

Supprimer les pièces jointes correspondantes

Cette action supprime toutes les pièces jointes qui correspondent aux critères de la règle. Elle entre dans la catégorie des actions de type Modifier (voir la rubrique *Actions Modifier* à la page 3-27).

Remarque : L'action Supprimer les pièces jointes correspondantes n'est applicable que lorsque les critères Taille, Pièce jointe, Contenu et/ou Virus sont utilisés dans la règle. Par exemple, une règle de spam avec une action de type Supprimer les pièces jointes correspondantes n'a pas d'incidence sur le message.

Pour configurer une action de règle afin de supprimer les pièces jointes qui correspondent à un critère :

1. Sélectionnez **Supprimer les pièces jointes correspondantes** à partir de la section Modifier.
2. Cliquez sur **Suivant** si vous créez une nouvelle règle ou sur **Enregistrer** si vous modifiez une règle existante.

Insérer un horodatage dans le corps du message

L'action Insérer l'horodatage insère un bloc de texte dans le corps du message. Les horodatages sont traités comme des objets nommés dans la base de données et sont sélectionnés à partir d'une liste. Les définitions d'horodatages contiennent le texte de l'horodatage (pouvant contenir des variables Hosted Email Security), que celui-ci soit inséré au début ou à la fin du corps du message et qu'il évite ou non l'horodatage de messages TNEF (Transport Neutral Encapsulation Format) ou signés numériquement pour éviter les ruptures.

Pour configurer une action de règle afin d'insérer un horodatage au corps du message :

1. Cochez la case **Insérer l'horodatage dans le corps**.
2. Cliquez sur **Modifier**. L'écran Horodatages apparaît, affichant une liste déroulante des horodatages disponibles.
3. Sélectionnez un horodatage dans la liste ou cliquez sur **Ajouter, Modifier,** ou **Copier** pour créer un nouvel horodatage ou modifier un horodatage existant.
4. Cliquez sur **Terminé**.

Baliser la ligne d'objet

L'action Baliser l'objet insère un texte configurable dans la ligne d'objet du message. Elle entre dans la catégorie des actions de type Modifier (voir la rubrique *Actions Modifier* à la page 3-27).

Pour configurer une action de règle afin de baliser l'objet du message :

1. Cochez la case **Baliser l'objet**.
2. Cliquez sur le lien balise pour ouvrir l'écran de modification du balisage.
3. Saisissez une balise dans le champ Balise.

4. Cochez ou décochez la case **Ne balisez pas les messages à signature numérique**.
5. Cliquez sur **Enregistrer**.

Envoyer un message de notification

Les notifications sont des messages envoyés lorsque la règle est déclenchée. Cette action entre dans la catégorie des actions de type Surveiller (voir la rubrique *Actions Surveiller* à la page 3-27).

Pour configurer un message de notification :

1. Dans la section Surveiller de l'écran Action, cochez la case **Envoyer une notification** et cliquez sur le lien **message à des personnes**.
2. Sélectionnez une notification existante et cliquez sur **Modifier** ou cliquez sur **Ajouter** pour créer un nouveau message de notification. L'écran Ajouter une règle > Notifications apparaît alors.
3. Donnez un nom à la notification.
4. Saisissez une adresse dans le champ **De**. Cette adresse apparaît dans le champ de l'expéditeur lorsque le message de notification est lu par les destinataires. Elle peut être utilisée pour dissimuler Hosted Email Security aux yeux des utilisateurs internes ou des destinataires externes.
5. Saisissez une adresse dans le champ **À**. Cette adresse est utilisée lorsque le message de notification est envoyé à l'administrateur.
6. Sélectionnez les destinataires de la notification :
   - Sélectionnez **Expéditeur** pour envoyer le message de notification à l'expéditeur.
   - Sélectionnez **Destinataire** pour envoyer le message de notification au destinataire. (Cette option n'est possible que si votre niveau de service le propose.)
   - Sélectionnez **Déroutement SNMP** pour envoyer une notification par SNMP. Si vous sélectionnez SNMP, sélectionnez également l'un des deux premiers boutons d'option et choisissez le code de catégorie approprié. (Cette option n'est possible que si votre niveau de service le propose.)
7. Saisissez un objet pour le message. Utilisez des variables si nécessaire.

8. Sélectionnez **Mettre en pièce jointe** pour mettre en pièce jointe une copie du message initial au message de notification et sélectionnez **Message modifié** ou **Message non modifié** dans la liste déroulante.

   AVERTISSEMENT ! Si elle est sélectionnée, l'option « Message non modifié » peut ouvrir la voie à des messages ou pièces jointes infectés dans votre environnement de messagerie. Trend Micro recommande vivement de ne pas choisir ce paramètre, sauf si vous devez analyser les messages dans leur forme non modifiée.

9. Saisissez le corps du message de notification dans le champ **Texte**. Cliquez sur le lien **Liste des variables** pour afficher les variables qu'il est possible d'utiliser dans les messages de notification.
10. Cliquez sur **Enregistrer**.

Copier en copie cachée (BCC) un autre destinataire

L'action BCC envoie une copie cachée (ou BCC, « blind carbone copy ») à un ou plusieurs destinataires configurés dans cette règle. Cette action entre dans la catégorie des actions de type Surveiller (voir la rubrique *Actions Surveiller* à la page 3-27).

Vous ne pouvez configurer d'envoi de notification qu'à une adresse de votre propre domaine.

Pour configurer une action de règle afin d'envoyer une copie du message à un destinataire BCC :

1. À partir de la section Surveiller de l'écran Action, cochez la case BCC.
2. Saisissez l'adresse électronique du destinataire dans le champ. Dans le cas de plusieurs adresses électroniques, saisissez-les dans le champ en les séparant par des virgules.
3. Si vous créez une nouvelle règle, cliquez sur **Suivant.** Si vous modifiez une règle existante, cliquez sur **Enregistrer.**

Rejeter le message

L'action de rejet bloque le message avec certains types de pièces jointes provenant du MTA en amont. Le message est enregistré comme rejeté dans les journaux Hosted Email Security, mais une fois rejeté, il n'est pas récupérable.

Remarque : L'action « Rejeter le message » est uniquement disponible dans le cas des stratégies qui protègent contre les virus ou programmes malveillants.

Pour configurer une action de règle Limitation de scan afin de rejeter un message :

1. Sélectionnez l'action **Rejeter** le message dans la section Limitation de scan.
2. Cliquez sur **Suivant** si vous créez une nouvelle règle ou sur **Enregistrer** si vous modifiez une règle existante.

Contourner une règle

L'action de contournement ignore la règle spécifiée, mais continue à vérifier le message par rapport aux autres règles de la stratégie. L'action est enregistrée comme contournée dans les journaux Hosted Email Security.

Remarque : L'action « Contourner cette règle » est uniquement disponible dans le cas des stratégies qui protègent contre les virus ou programmes malveillants.

Pour configurer une action de règle Limitation de scan afin de contourner un message :

1. Sélectionnez l'action **Contourner cette règle** dans la section Limitation de scan.

   AVERTISSEMENT ! Le message transmis peut contenir un risque au niveau de la sécurité.

2. Cliquez sur **Suivant** si vous créez une nouvelle règle ou sur **Enregistrer** si vous modifiez une règle existante.

Chiffrer des e-mails

Cette action de règle a pour objectif de protéger les données confidentielles contenues dans les e-mails envoyés par les utilisateurs au sein de votre entreprise. Le service Email Encryption exploite l'architecture existante de Hosted Email Security. Lorsque le contenu d'un e-mail active une règle de filtrage de contenu pour laquelle le chiffrement est actif, Hosted Email Security envoie le message au serveur de chiffrement Hosted Email Security qui chiffre l'e-mail et le transfère à l'ATM sortant.

Cette action est unique, dans la mesure où elle constitue une action non terminale ne pouvant pas coexister avec d'autres actions (terminales ou non terminales) de la même règle. Elle n'est applicable qu'aux règles sortantes.

Dans la plupart des cas, la règle permettant le chiffrement sera basée sur les éléments suivants :

- Les expéditeurs et destinataires des messages (par exemple, une règle chiffrant tous les messages envoyés des Ressources humaines au Service juridique)
- Le contenu du corps du message

Pour obtenir des instructions détaillées quant à l'utilisation des expressions à mot-clé avec le filtrage de contenu, consultez la rubrique *Filtrage de contenu* à partir de la page 3-6.

Pour configurer une règle et chiffrer les messages électroniques :

1. Dans le menu de gauche, cliquez sur **Stratégie**. L'écran « Stratégie » apparaît alors.
2. Cliquez sur **Ajouter**. L'écran Ajouter une règle / Étape 1 : Sélectionner les destinataires et les expéditeurs s'affiche.
3. Sélectionnez **Messages sortants** dans la liste déroulante « Cette règle s'applique à ».
4. Cliquez sur le lien **Expéditeurs** et sélectionnez une ou plusieurs adresses ou domaines.
5. Cliquez sur **Enregistrer** pour fermer la fenêtre, puis sur **Suivant** pour passer à l'étape 2 : Sélectionner l'écran des critères de scan.
6. Acceptez les paramètres par défaut (« Aucun critère ») ou cliquez sur **Avancé**. Plusieurs options s'affichent sous l'option Avancé.
7. Sélectionnez une option dans cette liste pour analyser le message à la recherche d'un contenu donné, par exemple, **L'objet correspond, Le corps correspond, L'en-tête spécifié correspond** ou **Le contenu de la pièce jointe correspond.**

8. Cliquez sur le lien « Expressions à mot-clé » à côté de l'option sélectionnée et ajoutez une ou plusieurs expressions à mot-clé (voir la rubrique *Filtrage de contenu* à partir de la page 3-6).
9. Cliquez sur **Suivant.** L'écran Ajouter une règle / Étape 3 : Sélectionner les actions s'affiche.
10. Acceptez la valeur par défaut « Ne pas intercepter les messages » et faites défiler jusqu'à la section « Modifier ».
11. Cochez la case **Chiffrer l'e-mail** et cliquez sur **Suivant**. L'écran Ajouter une règle / Étape 4 : L'écran Nom et Remarques s'affiche.
12. Entrez un nom pour la nouvelle règle et cliquez sur **Enregistrer**. Vous revenez à l'écran Stratégie dans laquelle la nouvelle règle est affichée en jaune.

Lecture d'un e-mail chiffré

Lorsqu'une règle de type « Chiffrer l'e-mail » est activée, il existe deux méthodes pour déchiffrer un message chiffré. La première consiste à acheter Trend Micro Email Encryption Client. Pour plus d'informations sur ce produit, consultez la page suivante sur le site Web Trend Micro :

http://fr.trendmicro.com/fr/products/enterprise/email-encryption/

Si vous n'utilisez pas ce client, le destinataire reçoit une notification similaire à la *figure 3-8* à la page 3-23.

Remarque : Il est impossible de déchiffrer le message chiffré à l'aide de Microsoft Outlook Web Access 2007.

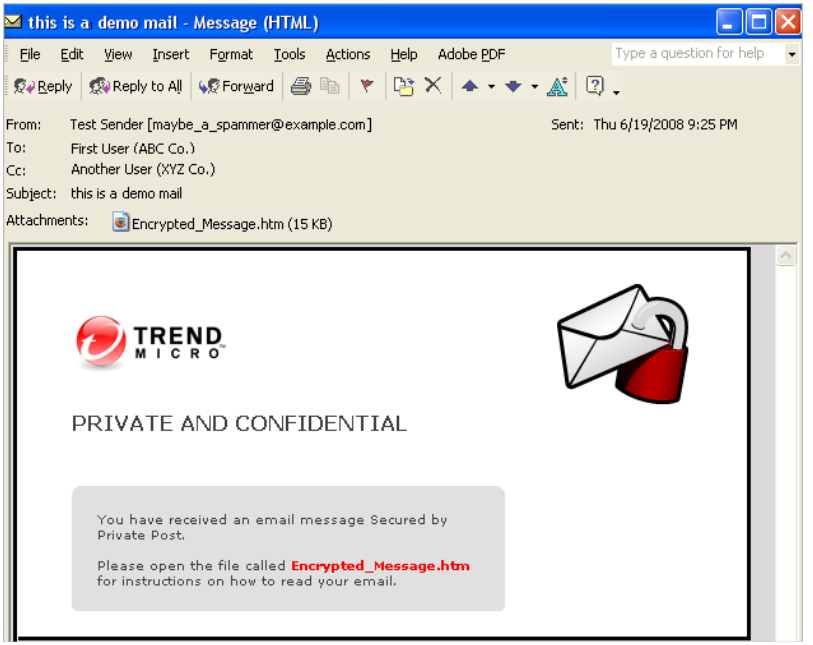

this is a demo mail - Message (HTML)
File Edit View Insert Format Tools Actions Help Adobe PDF
Type a question for help
Reply Reply to All Forward
From: Test Sender [maybe_a_spammer@example.com]
Sent: Thu 6/19/2008 9:25 PM
To: First User (ABC Co.)
Cc: Another User (XYZ Co.)
Subject: this is a demo mail
Attachments: Encrypted_Message.htm (15 KB)
TREND MICRO
PRIVATE AND CONFIDENTIAL
You have received an email message Secured by Private Post.
Please open the file called Encrypted_Message.htm for instructions on how to read your email.

FIGURE 3-8. Notification de message chiffré

Pour récupérer un e-mail chiffré, le destinataire doit suivre cette procédure :

1. Double-cliquez sur le fichier joint « Encrypted_Message.htm ». Celui-ci s'ouvre dans le navigateur par défaut de l'utilisateur, comme indiqué à la *figure 3-9*.

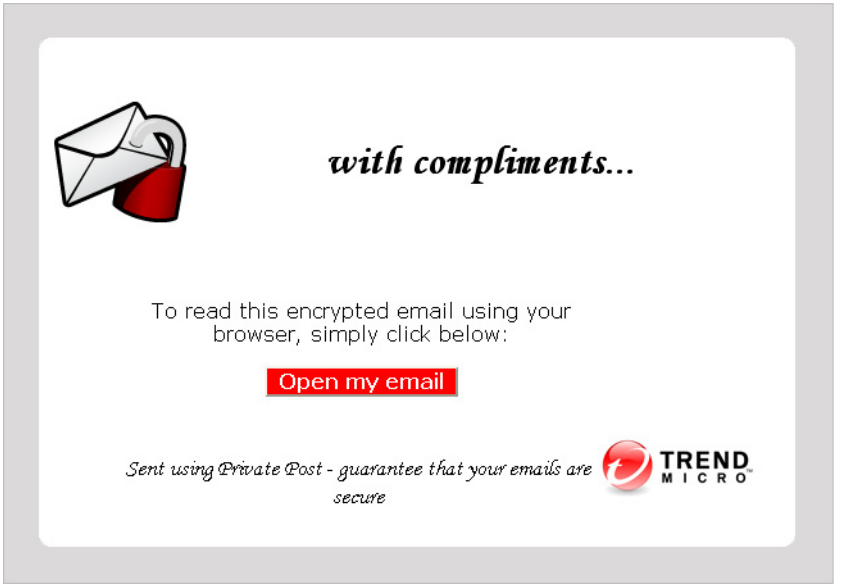

with compliments...
To read this encrypted email using your browser, simply click below:
Open my email
Sent using Private Post - guarantee that your emails are secure
TREND MICRO

FIGURE 3-9. Message_Crypté.htm visualisé dans le navigateur

2. Cliquez sur **Open my email** (Ouvrir l'e-mail) et, si vous n'êtes pas encore enregistré, indiquez les informations d'enregistrement dans les pages suivantes. Si vous êtes déjà enregistré auprès de ce service, le site de chiffrement affiche à ce stade l'e-mail déchiffré.

Remarque : La fonction « Open my email (Ouvrir l'e-mail) » peut ne pas fonctionner correctement avec certains systèmes de messagerie Web. Si le bouton ne fonctionne pas, le client peut enregistrer la pice jointe sur un ordinateur pour l'ouvrir.

---

3. Pour davantage de sécurité, trouvez une image de vérification CAPTCHA, tapez et confirmez une phrase secrète, sélectionnez trois questions de sécurité et répondez-y. Une fois l'enregistrement effectué, le site de chiffrement envoie un message d'activation au compte de messagerie du destinataire.
4. À la réception du message d'activation, cliquez sur **Please click here to validate your identity (Cliquez ici pour valider votre identité).** Le site de chiffrement d'e-mail Trend Micro se charge dans votre navigateur et affiche le message déchiffré, comme indiqué à la *figure 3-10* à la page 3-25.

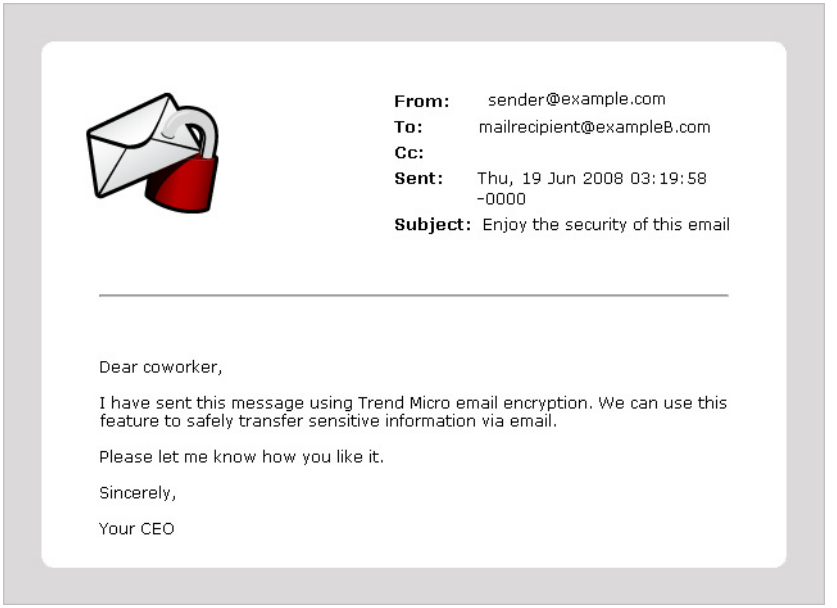

From: sender@example.com
To: mailrecipient@exampleB.com
Cc:
Sent: Thu, 19 Jun 2008 03:19:58 -0000
Subject: Enjoy the security of this email
Dear coworker,
I have sent this message using Trend Micro email encryption. We can use this feature to safely transfer sensitive information via email.
Please let me know how you like it.
Sincerely,
Your CEO

FIGURE 3-10. E-mail déchiffré

Remarque : Les destinataires ne doivent s'inscrire qu'une seule fois. Après l'inscription au service Email Encryption, le destinataire pourra afficher le message déchiffré dans le navigateur en cliquant simplement sur **Open my email (Ouvrir l'e-mail)**.

Ordre d'exécution des règles

Toutes les règles sont organisées automatiquement pour des raisons de sécurité et d'efficacité d'exécution. Les administrateurs n'ont pas à déterminer l'ordre d'exécution des règles. Il existe quatre types d'actions dans une règle :

- *Actions Intercepter*
- *Actions Modifier*
- *Actions Surveiller*
- *Limitations de scan*
- *Action Chiffrement d'e-mail*

Actions Intercepter

Une fois qu'une action Intercepter ou « terminale » s'exécute, le traitement de cette règle s'arrête et aucune action supplémentaire n'est mise en œuvre pour cette règle.

Les actions Intercepter exécutent ce qui suit dans un ordre de priorité strict:

1. Supprimer le message entier
2. Envoyer le message maintenant (voir la remarque à la page 3-32)
3. Mettre le message en quarantaine
4. Réexpédier à un autre destinataire

Remarque importante sur l'action Envoyer maintenant

L'action « Envoyer maintenant » n'est pas recommandée comme action unique. Si vous choisissez « Envoyer maintenant » en tant qu'action unique pour les messages de spam, par exemple, tous ces messages seront simplement envoyés à vos destinataires, comme si aucun filtre anti-spam n'était en place.

Si vous utilisez « Envoyer maintenant » avec une règle de virus, vérifiez que vous avez également configuré une action « Supprimer » pour la règle de virus. Seule l'action « Supprimer » dispose d'un degré de priorité supérieur à l'action « Envoyer maintenant », et elle sera donc traitée avant cette dernière (puis mettra fin au traitement de cette règle).

AVERTISSEMENT ! Si vous choisissez « Envoyer maintenant » en tant qu'action unique pour une règle de virus, les e-mails contenant des virus pourraient s'infiltrer sans être bloqués.

Actions Modifier

Les actions « Modifier » (non terminales) suivantes s'exécutent mais ne mettent pas fin au traitement (l'e-mail sera envoyé aux destinataires initialement souhaités) :

- Nettoyer les virus nettoyables
- Supprimer la pièce jointe
- Insérer un horodatage dans le corps du message
- Baliser la ligne d'objet

Conseil : Les actions Intercepter (« terminales ») ont une priorité d'exécution plus importante que les actions non terminales. Lorsqu'une action terminale est déclenchée, aucune autre action n'est ncessaire. Cependant, les actions non terminales peuvent être combinées, par exemple « Supprimer une pièce jointe » et « Horodater le corps du message ».

Actions Surveiller

Il existe deux actions de surveillance :

- Envoyer un message de notification
- Copier en copie cachée (BCC) un autre destinataire

Vous pouvez combiner la première action avec tout autre type d'action. Vous pouvez combiner l'action BCC avec des actions « Modifier » (et avec la première action « Surveiller »). Cependant, l'action BCC ne peut pas être combinée avec les actions terminales (intercepter).

Conseil : Le message électronique de notification envoyé pour surveiller les actions peut être personnalisé en utilisant les variables expliquées dans l'aide en ligne.

Limitations de scan

Il existe deux déclencheurs de limitation de scan :

- Le fichier Office 2007 contient plus de 353 fichiers.
- L'archive compressée contient plus de 353 fichiers.

- Le fichier Office 2007/2010 contient un fichier dont le taux de décompression est supérieur à 100.
- Le fichier compressé contient un fichier dont le taux de décompression est supérieur à 100.

Les limitations de scan sont uniquement utilisables avec des stratégies qui protègent contre les virus ou programmes malveillants. Elles peuvent être combinées avec les actions terminales ou de type Modifier.

Action Chiffrement d'e-mail

Cette fonction n'est disponible que pour les utilisateurs de Hosted Email Security.

L'action Chiffrer des e-mails de Trend Micro est disponible si vous avez acheté ce service complémentaire. Le service Email Encryption est uniquement accessible aux clients de Hosted Email Security ayant activé le filtrage sortant. Cette action est unique, dans la mesure où elle constitue une action non terminale ne pouvant pas coexister avec d'autres actions (terminales ou non terminales) de la même règle. Si plusieurs règles s'appliquent à un message, Hosted Email Security traite la règle de chiffrement après toutes les autres.

Remarque : Notez que « ne pas intercepter » n'est pas considéré comme une action.

Ajout et modification de règles

Seuls les utilisateurs de Hosted Email Security peuvent ajouter, modifier, copier ou supprimer des règles. Pour des instructions détaillées, consultez les sections ci-dessous.

Ajout d'une nouvelle règle

Les règles sont le moyen par lequel les stratégies de messagerie sont appliquées au trafic de messagerie dans Hosted Email Security. Chaque règle se compose de trois parties principales :

- Le(s) utilisateur(s) ou le(s) domaine(s) au(x)quel(s) la règle s'applique.
- Les critères évalués pour déterminer si la règle doit être déclenchée.
- L'action que Hosted Email Security effectuera si la règle est activée.

Une fois ces trois parties d'une règle configurées, vous devez attribuer un nom unique à la règle pour l'identifier dans les résumés, les suivis des messages et partout ailleurs. Vous pouvez désactiver une règle sans perdre sa configuration, puis la réactiver ultérieurement.

Pour créer une règle :

1. Cliquez sur **Ajouter** dans l'écran Stratégie. L'écran **Ajouter une règle** apparaît alors.

FIGURE 3-11. Écran Ajouter une règle

2. Sélectionnez le(s) utilisateur(s) ou le(s) domaine(s) au(x)quel(s) la règle s'applique.

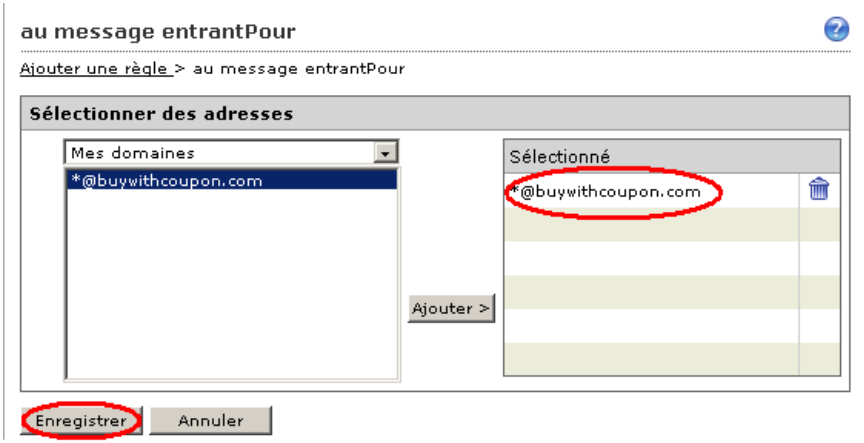


FIGURE 3-12. Ajoutez les domaines et les utilisateurs sur cet écran.

3. Sélectionnez et configurez les critères.

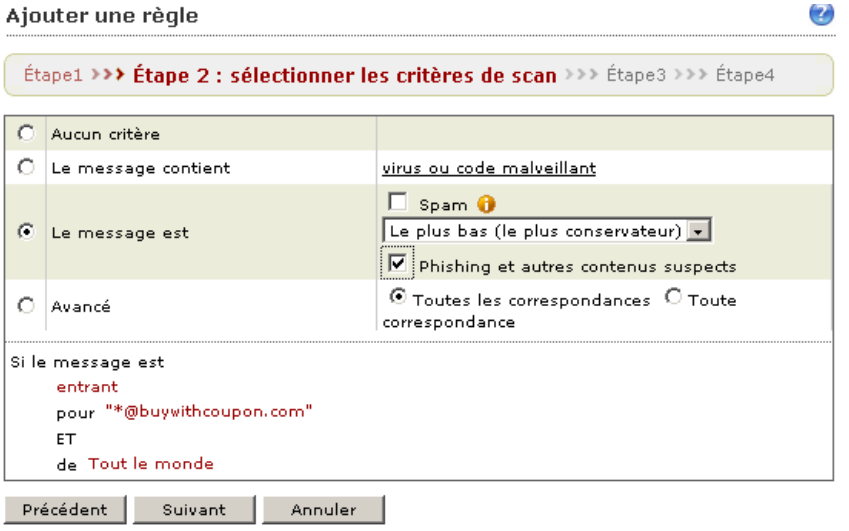


FIGURE 3-13. Sélectionnez les critères pour la règle sur cet écran.

4. Sélectionnez et configurez les actions Intercepter.

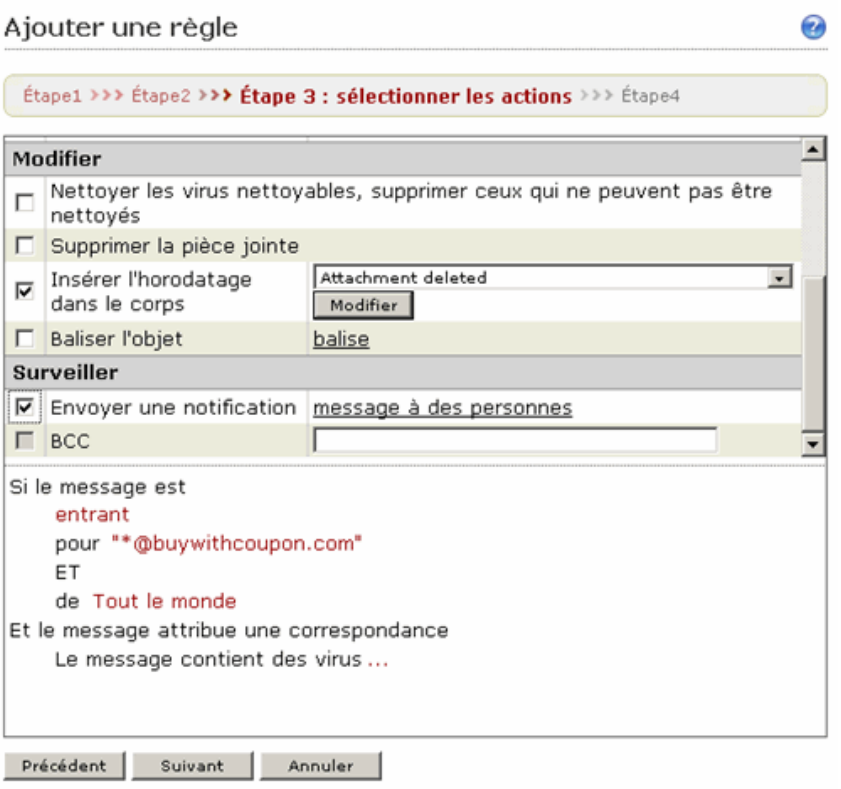


FIGURE 3-14. Sélectionnez les actions sur cet écran

AVERTISSEMENT ! L'action « Envoyer maintenant » n'est pas recommandée pour être utilisée comme action unique. Lorsqu'elle est sélectionnée, l'action « Envoyer maintenant » contourne toutes les autres règles. C'est pourquoi, si vous avez des critères à rechercher, ils ne seront pas traités.

Si vous choisissez « Envoyer maintenant » en tant qu'action unique pour les messages de spam, par exemple, tous ces messages seront simplement envoyés à vos destinataires, comme si aucun filtre anti-spam n'était en place.

Si vous choisissez « Envoyer maintenant » en tant qu'action unique pour une règle de virus, les e-mails contenant des virus pourraient s'infiltrer sans être bloqués.

Si vous tentez de définir « Envoyer maintenant » en tant qu'action, le message d'avertissement *figure 3-15* ci-dessous apparaît.

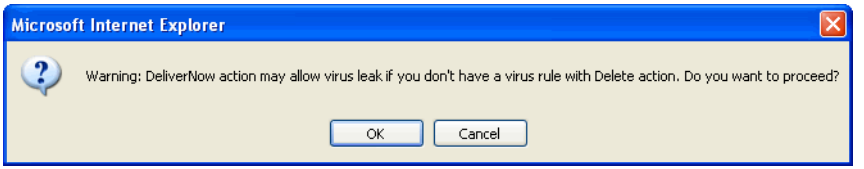

Microsoft Internet Explorer
Warning: DeliverNow action may allow virus leak if you don't have a virus rule with Delete action. Do you want to proceed?
OK
Cancel

FIGURE 3-15. Message d'avertissement Envoyer maintenant

5. De façon facultative, sélectionnez une action Modifier ou Surveiller, tel que décrit dans la *figure 3-16* ci-dessous.

   Vous pouvez également sélectionner des actions Limitation de scan pour les stratégies antivirus.

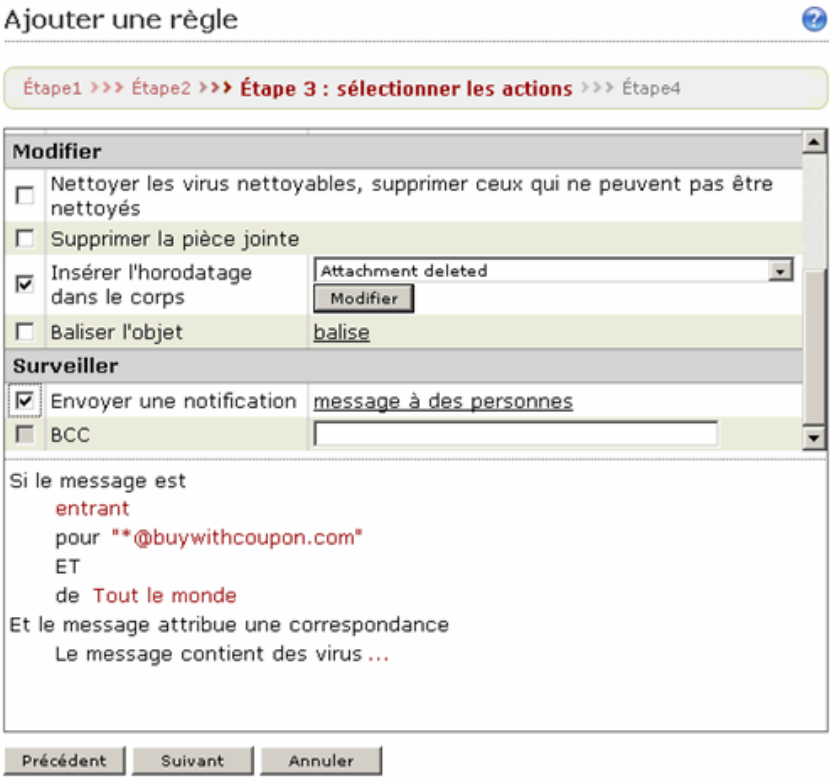


FIGURE 3-16. Étape 3 : sélection des actions Modifier et Surveiller

6. Nommez et activez la règle.

FIGURE 3-17. Nommez et enregistrez la règle sur cet écran

7. Cliquez sur **Enregistrer**.

   L'écran **Stratégie** s'affiche et présente votre nouvelle règle dans l'ordre approprié, mise en surbrillance dans la liste, comme indiqué dans la *figure 3-18* ci-dessous.

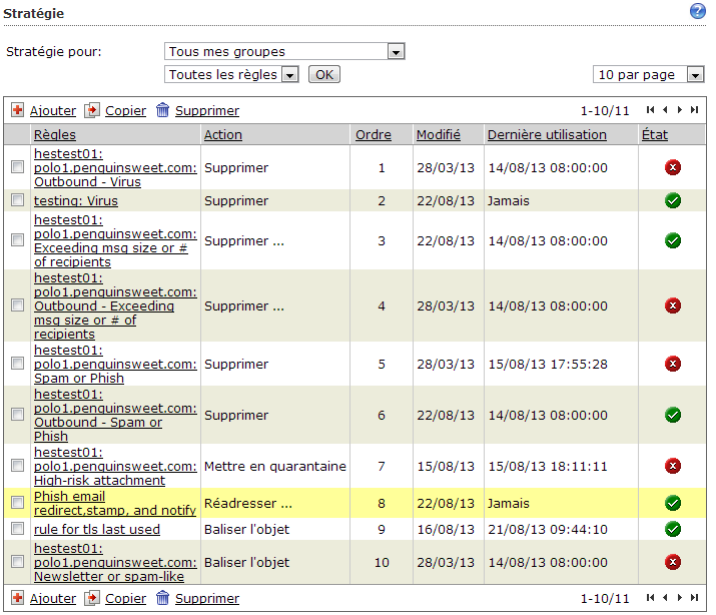


FIGURE 3-18. L'écran Stratégie affiche la stratégie nouvellement créée

Modification d'une règle existante

Pour modifier une règle existante :

1. Dans la liste des règles, cliquez sur le nom de la règle que vous souhaitez modifier.
2. Modifiez la règle.

   L'exemple ci-dessous indique comment ajouter un destinataire approuvé à cette règle.

   a. Cliquez sur le lien **Si le message est…** pour modifier la liste d'exceptions des expéditeurs.

   b. Cliquez sur **Exception** sur la ligne de l'expéditeur.

   c. Saisissez l'adresse de l'expéditeur dans la zone de texte pour ajouter un expéditeur approuvé à la liste d'exceptions.

      Dans l'exemple de la *figure 3-19* à la page 3-36, « ceo@example.com » a été exclu de cette règle.
3. Cliquez sur **Enregistrer** pour sauvegarder les expéditeurs approuvés pour cette règle. Cela enregistre les expéditeurs approuvés mais non la règle.

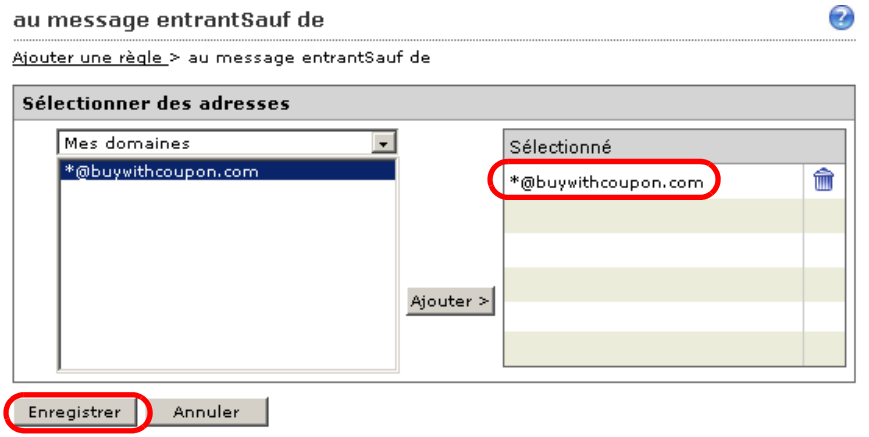


FIGURE 3-19. Modifiez les exceptions relatives aux expéditeurs sur cet écran.

4. Cliquez sur **Enregistrer** pour continuer.

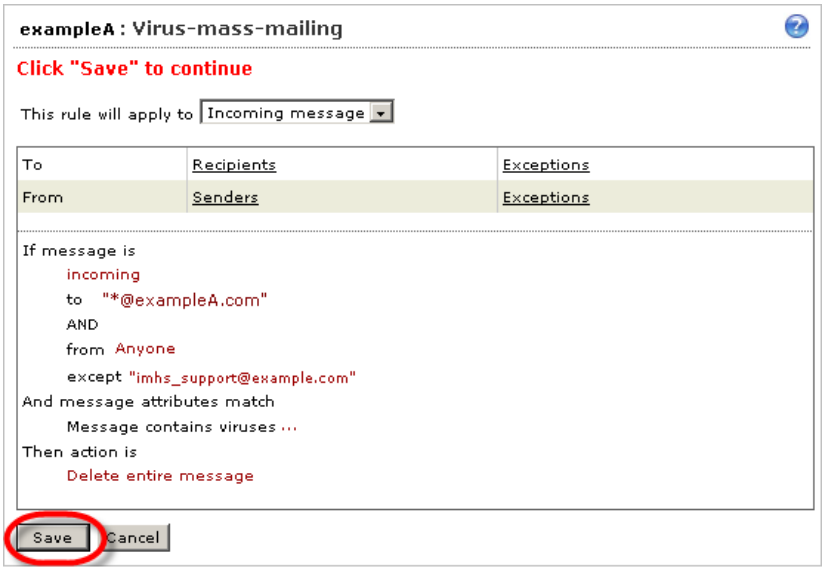


FIGURE 3-20. Écran de modification de la stratégie

5. Cliquez de nouveau sur **Enregistrer** pour sauvegarder la règle.

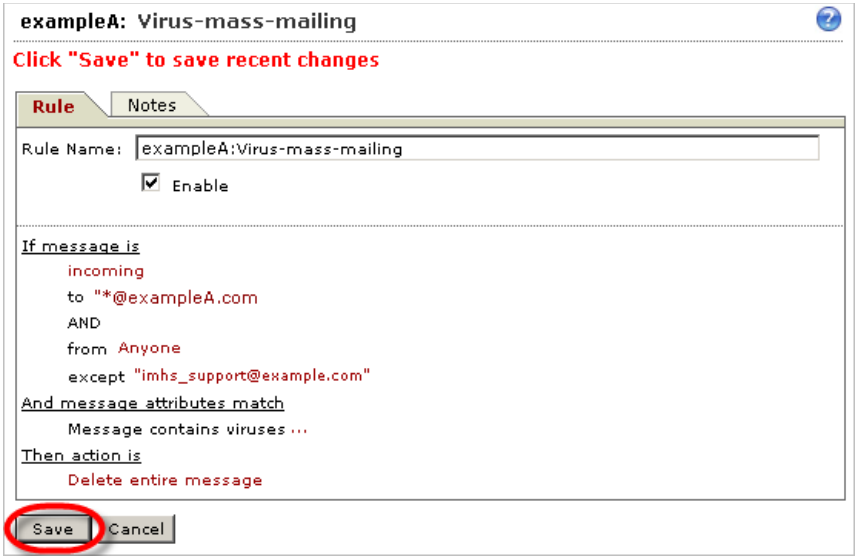


FIGURE 3-21. Enregistrez les modifications apportées à la stratégie sur cet écran

Copie d'une règle existante

Souvent, les nouvelles règles sont très semblables aux règles existantes. Dans de tels cas, il est généralement plus facile de copier la règle, puis de modifier la copie, plutôt que de créer une nouvelle règle depuis le début.

Pour copier une règle existante :

1. Dans la liste des règles, cochez la case en regard de la règle à copier.
2. Cliquez sur **Copier**. Une règle nommée « Copie de [nom original de la règle] » apparaît dans la liste des règles.
3. Modifiez la règle.

Suppression d'une règle existante

Pour supprimer des règles existantes :

1. Dans la liste des règles, cochez la case en regard de la règle à supprimer.
2. Cliquez sur **Supprimer**.

Chapitre 4

Expéditeurs approuvés, quarantaine et journaux

Ce chapitre explique comment définir des expéditeurs approuvés, accéder à la quarantaine, utiliser l'e-mail d'aperçu des spams, utiliser Web End User Quarantine et interpréter les journaux de Hosted Email Security.

Sujets abordés dans ce chapitre :

- *Expéditeurs approuvés* à la page 4-2
- *Quarantaine* à la page 4-3
- *Web End-User Quarantine* à la page 4-13
- *Journaux* à la page 4-14

Expéditeurs approuvés

L'écran Expéditeurs approuvés permet aux administrateurs de messagerie d'approuver des adresses électroniques ou des domaines spécifiques, qui pourront envoyer des messages aux domaines gérés.

Remarque : Cet écran est distinct des listes de réputation IP approuvées/bloquées (**Réputation IP > Approuvés/Bloqués**). Dans cet écran, vous pouvez approuver les adresses électroniques ou les domaines de façon qu'ils ne soient pas scannés ; l'écran Approuvés/Bloqués sous Réputation IP s'applique exclusivement aux contrôles de réputation IP.

Pour les expéditeurs approuvés :

- Hosted Email Security ne bloquera aucun message provenant des expéditeurs (ou domaines) spécifiés
- Les règles heuristiques anti-spam basées sur le contenu ne s'appliqueront pas aux e-mails envoyés par les expéditeurs ou domaines spécifiés
- Toutes les règles antivirus, basées sur le contenu et relatives aux pièces jointes s'appliqueront

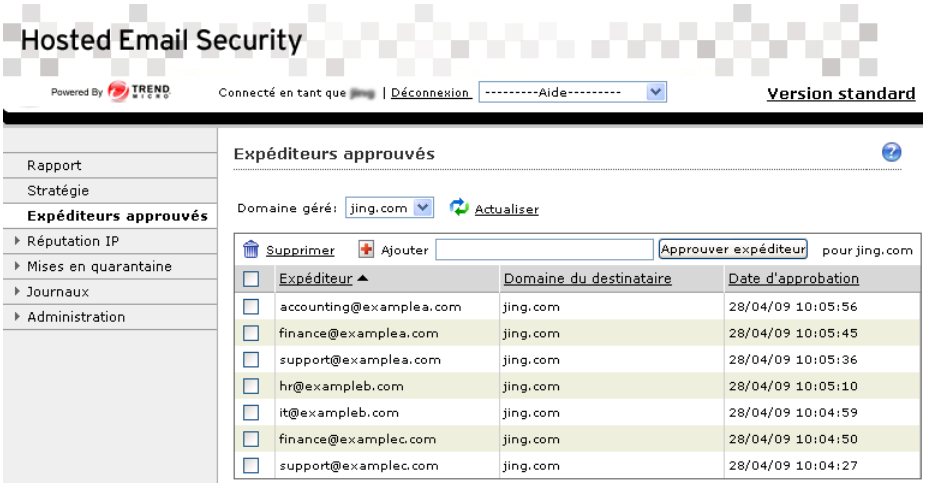


FIGURE 4-1. Écran Expéditeurs approuvés

Pour ajouter des expéditeurs approuvés :

1. Dans la liste déroulante Domaine géré, sélectionnez le domaine spécifique (ou Tous les domaines) auquel les expéditeurs approuvés seront ajoutés.
2. Cliquez sur **Actualiser**.
3. Entrez une adresse ou un domaine unique dans le champ **Ajouter**.

   Exemple :

   - Pour une adresse unique, entrez : nom@exemple.com
   - Pour un domaine, entrez : *@exemple.com
4. Cliquez sur **Approuver expéditeur**.

Pour modifier une entrée de liste :

1. Cliquez sur l'entrée.
2. Apportez les modifications.
3. Cliquez sur **OK**.

Pour supprimer une entrée :

1. Cochez la case de cette entrée.
2. Cliquez sur **Supprimer**.

Quarantaine

Cette section ne vous concerne que si votre niveau de service autorise cette fonctionnalité.

Demande de mise en quarantaine

Cet écran affiche la liste de tous les messages en quarantaine qui répondent à vos critères de demande. Il fournit également les outils permettant de gérer ces messages.

Pour supprimer un ou plusieurs messages de la quarantaine :

1. Cochez la case correspondant au(x) message(s) à supprimer.
2. Cliquez sur **Supprimer** pour effacer les messages sélectionnés de manière permanente.

Pour transmettre un ou plusieurs messages à partir de la quarantaine :

1. Cochez la case correspondant au(x) message(s) à renvoyer.
2. Cliquez sur **Transmettre (non spam)** pour libérer les messages sélectionnés de la quarantaine.

Remarque : Si vous cliquez sur **Transmettre (Non spam)**, les messages sélectionnés sont libérés de la quarantaine, puis traités par Hosted Email Security (sauf que cette fois, le critère anti-spam n'est pas appliqué). Cependant, il se peut que ces messages n'arrivent pas dans votre boîte de réception s'ils enfreignent d'autres stratégies de sécurité de la messagerie d'entreprise.

Pour supprimer ou transmettre tous les messages de la liste :

1. Cochez la case en regard de l'en-tête de colonne **Date** pour sélectionner tous les messages. Hosted Email Security sélectionne tous les messages à l'écran.
2. Cliquez sur **Supprimer** ou **Transmettre (non spam)**. Hosted Email Security supprime tous les messages de la liste.

Paramètres de l'option Mettre en quarantaine

Dans l'écran des paramètres de l'option Mettre en quarantaine (Figure 4-2), vous pouvez configurer un e-mail d'aperçu récapitulatif qui répertorie jusqu'à 100 messages de l'utilisateur final mis en quarantaine. Cet e-mail fournit un lien permettant au titulaire du compte d'accéder aux messages qui l'intéressent. Vous pouvez également autoriser le titulaire du compte à approuver les messages en quarantaine depuis l'e-mail d'aperçu, comme indiqué ci-après.

Approbation de messages ou d'expéditeurs depuis l'e-mail d'aperçu des spams (action en ligne)

Dans l'écran des paramètres de l'option Mettre en quarantaine, vous pouvez activer l'action en ligne depuis l'e-mail d'aperçu des spams. Les destinataires de cet e-mail ont ainsi la possibilité d'approuver un ou plusieurs messages ou destinataires directement depuis l'e-mail au moyen d'un formulaire HTML.

Configuration de l'action en ligne pour l'aperçu des spams

En activant cette fonction, vous évitez aux utilisateurs de se connecter à End User Quarantine et d'approuver manuellement les messages ou les expéditeurs mis en quarantaine.

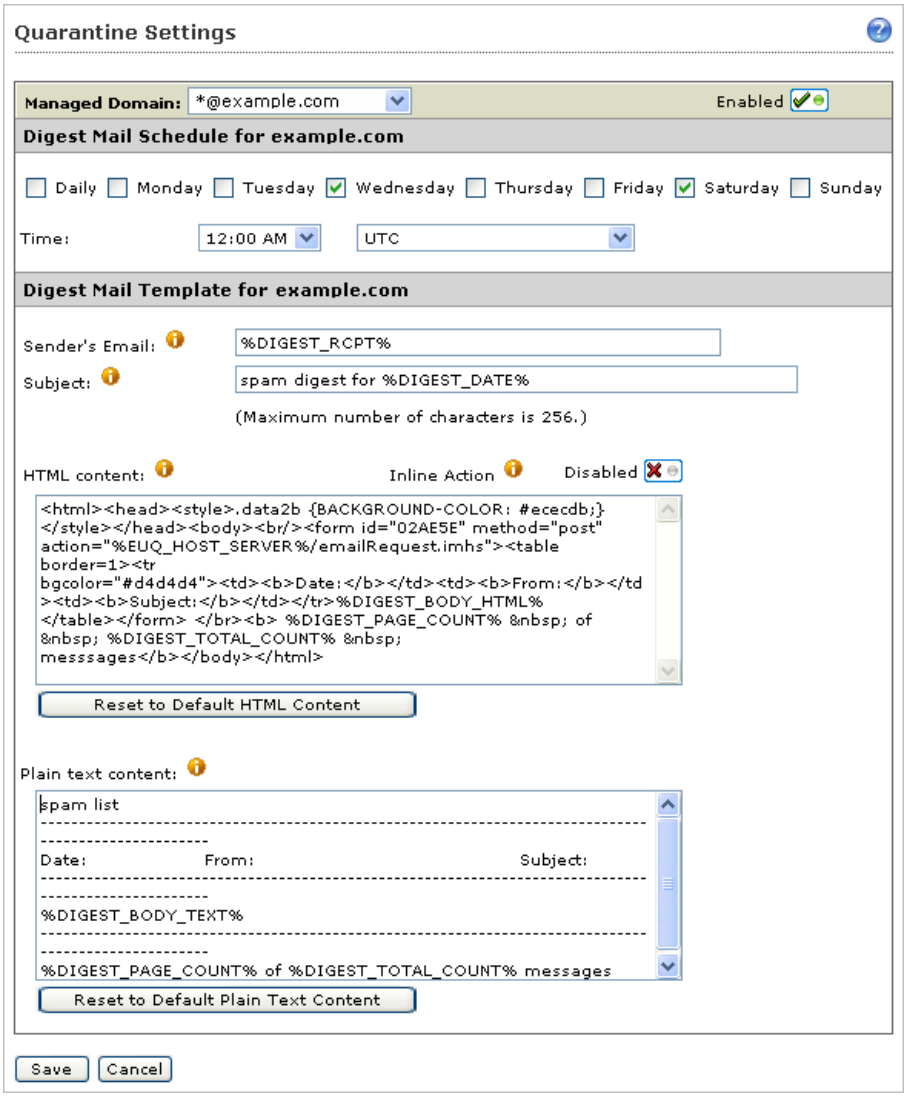


FIGURE 4-2. Paramètres de l'option Mettre en quarantaine permettant de configurer le message d'aperçu des spams

Pour configurer l'e-mail d'aperçu des spams :

1. Dans le menu de gauche, cliquez sur **Mises en quarantaine > Paramètres**. L'écran des paramètres de l'option Mettre en quarantaine s'affiche.
2. Dans l'angle supérieur droit de l'écran, cliquez sur l'icône **Désactivé** pour activer la fonction d'aperçu des spams. (Elle est désactivée par défaut.)
3. Sélectionnez le domaine géré pour lequel l'e-mail d'aperçu des spams sera créé.
4. Sélectionnez la fréquence d'envoi de l'e-mail d'aperçu des messages en quarantaine :
   - Quotidiennement
   - À des jours spécifiques. Par exemple, cochez les cases Lundi, Mercredi et Vendredi pour un envoi ces jours-là uniquement.

Remarque : Les e-mails mis en quarantaine sont conservés dans la quarantaine Hosted Email Security accessible sur le Web pendant 21 jours dans la région EMEA et pendant 15 jours dans toutes les autres régions.

---

5. Sélectionnez une heure et un fuseau horaire pour l'envoi de l'e-mail d'aperçu.
6. Définissez les éléments suivants pour l'e-mail d'aperçu :
   - **Adresse e-mail de l'expéditeur** : adresse électronique qui apparaîtra dans la ligne « De » de l'e-mail d'aperçu.
   - **Objet** : texte qui apparaîtra dans la ligne d'objet de l'e-mail d'aperçu.
   - **HTML content** (Contenu HTML) : contenu qui apparaîtra si le client de messagerie de l'utilisateur final autorise les e-mails en HTML. (Voir *figure 4-4*.)
   - **Plain text content** (Contenu en texte brut) : contenu qui apparaîtra si le client de messagerie de l'utilisateur final autorise uniquement les e-mails en texte brut. (Voir *figure 4-3*.)
7. Le cas échéant, cliquez avec le bouton droit sur chaque champ pour afficher un menu contextuel dans lequel sélectionner les jetons disponibles. Voir la description des jetons disponibles dans le *tableau 4-1*.

Remarque : Le domaine utilisé dans l'adresse électronique de l'expéditeur doit être identique au domaine auquel l'e-mail sera envoyé.

TABLEAU 4-1. Variables pour le modèle d'e-mail d'aperçu

CHAMP	JETONS DISPONIBLES	UTILISATION DE CE JETON...
E-mail de l'expéditeur	%DIGEST_RCPT%	L'adresse électronique du destinataire de l'aperçu apparaît dans le champ De : de l'e-mail d'aperçu reçu.
Objet	%DIGEST_RCPT%	L'adresse électronique du destinataire de l'aperçu apparaît dans la ligne d'objet.
	%DIGEST_DATE%	La date d'aperçu apparaît dans la ligne d'objet.
Contenu HTML	%DIGEST_RCPT%	L'adresse électronique du destinataire de l'aperçu apparaît dans le corps du message au format HTML.
	%DIGEST_DATE%	La date d'aperçu apparaît dans le corps HTML du message.
	%DIGEST_BODY_HTML%	Le résumé d'aperçu sous forme de tableau HTML apparaît dans le corps HTML du message.
	%DIGEST_TOTAL_COUNT%	Le nombre total de messages actuellement en quarantaine apparaît dans le corps HTML de l'e-mail d'aperçu.
	%DIGEST_PAGE_COUNT%	Le nombre total de messages en quarantaine dans le résumé d'aperçu sous forme de liste (jusqu'à 100 entrées) apparaît dans le corps HTML de l'e-mail d'aperçu.

TABLEAU 4-1. Variables pour le modèle d'e-mail d'aperçu (Suite)

CHAMP	JETONS DISPONIBLES	UTILISATION DE CE JETON...
Plain Text Content (Contenu en texte brut)	%DIGEST_RCPT%	L'adresse électronique du destinataire de l'aperçu apparaît dans le corps du message au format texte.
	%DIGEST_DATE%	La date d'aperçu apparaît dans le corps du message au format texte.
	%DIGEST_BODY_TEXT%	Le résumé d'aperçu en texte brut apparaît dans le corps du message au format texte.
	%DIGEST_TOTAL_COUNT%	Le nombre total de messages actuellement en quarantaine apparaît en texte brut dans le corps de l'e-mail d'aperçu.
	%DIGEST_PAGE_COUNT%	Le nombre total de messages en quarantaine répertoriés dans le résumé d'aperçu (jusqu'à 100 entrées) apparaît dans le corps en texte brut de l'e-mail d'aperçu.

8. Le cas échéant, cliquez sur l'icône « Désactivé » ( ) en regard de « Inline Action » (Action en ligne) au-dessus de la zone de texte de contenu HTML pour activer l'action en ligne, comme indiqué dans *Approbation de messages ou d'expéditeurs depuis l'e-mail d'aperçu des spams (action en ligne)* à la page 4-4. L'icône se transforme en Activé ( ) et l'aperçu des spams envoyé contient des boutons radio ainsi que des boutons Envoyer permettant à l'utilisateur d'approuver les messages ou les expéditeurs directement depuis l'e-mail d'aperçu des spams.
9. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

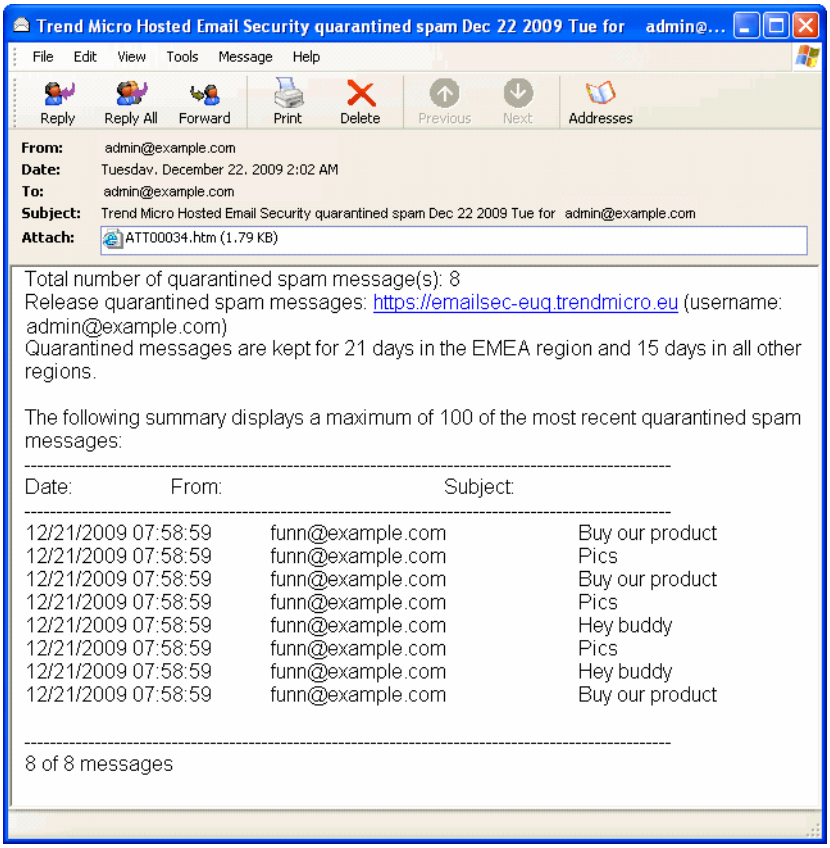

Trend Micro Hosted Email Security quarantined spam Dec 22 2009 Tue for admin@...
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: admin@example.com
Date: Tuesday, December 22, 2009 2:02 AM
To: admin@example.com
Subject: Trend Micro Hosted Email Security quarantined spam Dec 22 2009 Tue for admin@example.com
Attach: ATT00034.htm (1.79 KB)
Total number of quarantined spam message(s): 8
Release quarantined spam messages: https://emailsec-eug.trendmicro.eu (username: admin@example.com)
Quarantined messages are kept for 21 days in the EMEA region and 15 days in all other regions.
The following summary displays a maximum of 100 of the most recent quarantined spam messages:
Date: From: Subject:
12/21/2009 07:58:59 funn@example.com Buy our product
12/21/2009 07:58:59 funn@example.com Pics
12/21/2009 07:58:59 funn@example.com Buy our product
12/21/2009 07:58:59 funn@example.com Pics
12/21/2009 07:58:59 funn@example.com Hey buddy
12/21/2009 07:58:59 funn@example.com Pics
12/21/2009 07:58:59 funn@example.com Hey buddy
12/21/2009 07:58:59 funn@example.com Buy our product
8 of 8 messages

FIGURE 4-3. Exemple d'e-mail d'aperçu au format texte brut

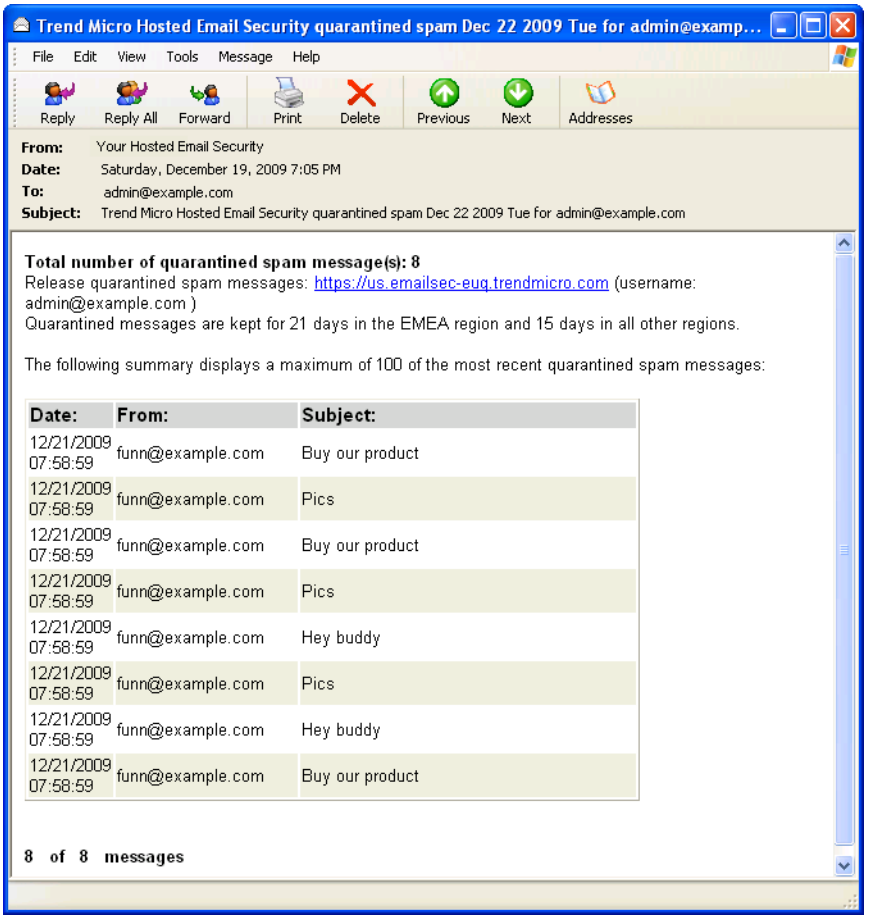

Trend Micro Hosted Email Security quarantined spam Dec 22 2009 Tue for admin@examp...
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: Your Hosted Email Security
Date: Saturday, December 19, 2009 7:05 PM
To: admin@example.com
Subject: Trend Micro Hosted Email Security quarantined spam Dec 22 2009 Tue for admin@example.com
Total number of quarantined spam message(s): 8
Release quarantined spam messages: https://us.emailsec-euq.trendmicro.com (username: admin@example.com)
Quarantined messages are kept for 21 days in the EMEA region and 15 days in all other regions.
The following summary displays a maximum of 100 of the most recent quarantined spam messages:
Date: From: Subject:
12/21/2009 07:58:59 funn@example.com Buy our product
12/21/2009 07:58:59 funn@example.com Pics
12/21/2009 07:58:59 funn@example.com Buy our product
12/21/2009 07:58:59 funn@example.com Pics
12/21/2009 07:58:59 funn@example.com Hey buddy
12/21/2009 07:58:59 funn@example.com Pics
12/21/2009 07:58:59 funn@example.com Hey buddy
12/21/2009 07:58:59 funn@example.com Buy our product
8 of 8 messages

FIGURE 4-4. Exemple d'e-mail d'aperçu HTML avec l'action en ligne désactivée (liste réduite à des fins de lisibilité)

Utilisation de l'action en ligne pour l'aperçu des spams

Puisqu'elle vous évite de devoir vous connecter au site End User Quarantine, l'action en ligne pour l'aperçu des spams vous permet de gagner du temps. Plusieurs points doivent être pris en compte lors de l'utilisation de cette fonction en présence d'un client de messagerie :

1. L'action en ligne d'aperçu des spams est uniquement compatible avec les ordinateurs présentant la configuration suivante :
   - Microsoft Office XP, service pack 3
   - Microsoft Outlook 2003 (SP3) ou Outlook Express 6.0
2. Si vous cliquez sur l'hyperlien au niveau de l'objet du message, le navigateur s'affichera et vous accéderez à la fenêtre de connexion au site EUQ.
3. Si vous envoyez le message avec l'option « Non spam », celui-ci ne sera pas placé en quarantaine. Si le message ne respecte pas plusieurs règles d'analyse, il est possible qu'en cas de nouveau traitement, celui-ci déclenche une règle autre que celle pour laquelle il avait été placé en quarantaine au départ. Le message sera donc à nouveau placé en quarantaine.
4. L'activation de l'option « Approuver l'expéditeur (Non spam) » lors de l'envoi du message permet de récupérer le message placé en quarantaine mais aussi d'ajouter l'expéditeur à la liste des expéditeurs approuvés.
5. Après avoir récupéré le message en quarantaine via l'option « Non spam », si vous renvoyez par la suite le même message en sélectionnant l'option « Approuver l'expéditeur (Non spam) », Hosted Email Security n'ajoutera pas l'expéditeur à la liste des expéditeurs approuvés parce que le message ne se trouve pas en quarantaine. Par conséquent, Hosted Email Security est incapable d'identifier l'expéditeur. Le message de réponse sera toutefois inchangé :

   ```
   Hosted Email Security a reçu votre demande de
   révision de l'état de spam d'un ou plusieurs
   messages ou expéditeurs.
   ```

6. Dernier point, et sans doute l'un des plus importants :

AVERTISSEMENT ! Toute personne recevant cet e-mail d'aperçu des spams pourra ajouter l'un de ces expéditeurs à votre liste des expéditeurs approuvés. Par conséquent, Trend Micro vous déconseille de transférer cet e-mail à un autre utilisateur.

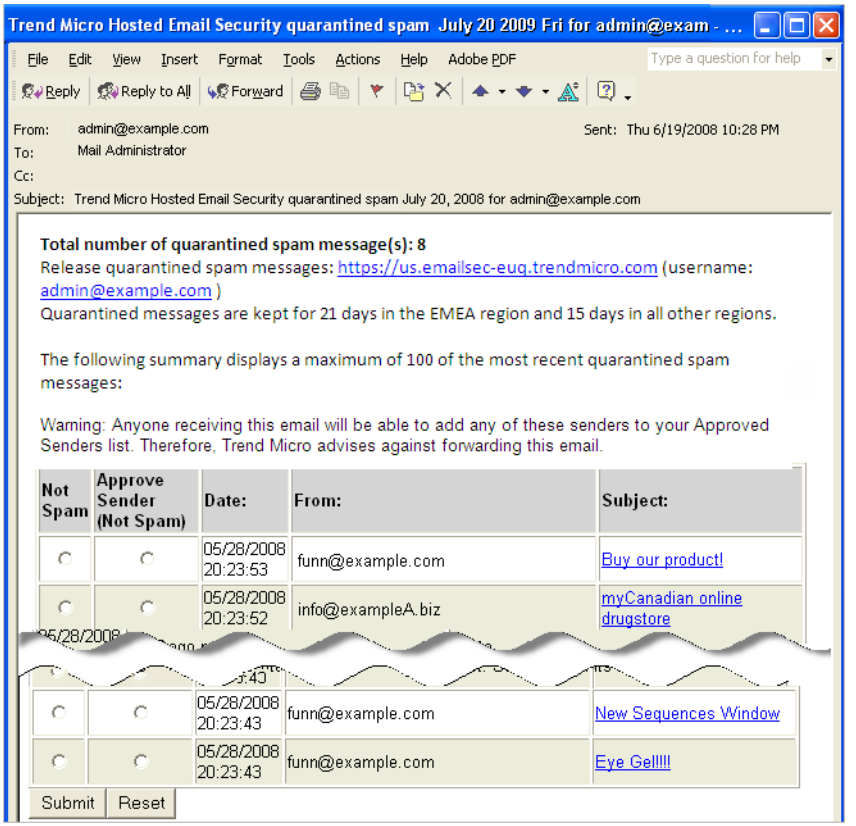

Trend Micro Hosted Email Security quarantined spam July 20 2009 Fri for admin@exam - ...
File Edit View Insert Format Tools Actions Help Adobe PDF
Type a question for help
Reply Reply to All Forward
From: admin@example.com
Sent: Thu 6/19/2008 10:28 PM
To: Mail Administrator
Cc:
Subject: Trend Micro Hosted Email Security quarantined spam July 20, 2008 for admin@example.com
Total number of quarantined spam message(s): 8
Release quarantined spam messages: https://us.emailsec-euq.trendmicro.com (username: admin@example.com)
Quarantined messages are kept for 21 days in the EMEA region and 15 days in all other regions.
The following summary displays a maximum of 100 of the most recent quarantined spam messages:
Warning: Anyone receiving this email will be able to add any of these senders to your Approved Senders list. Therefore, Trend Micro advises against forwarding this email.
Not Spam
Approve Sender (Not Spam)
Date:
From:
Subject:
05/28/2008 20:23:53
funn@example.com
Buy our product!
05/28/2008 20:23:52
info@exampleA.biz
myCanadian online drugstore
05/28/2008 20:23:43
funn@example.com
New Sequences Window
05/28/2008 20:23:43
funn@example.com
Eye Gel!!!!
Submit
Reset

FIGURE 4-5. Exemple d'e-mail d'aperçu HTML avec l'action en ligne désactivée (tronqué à des fins de lisibilité)

Web End-User Quarantine

Hosted Email Security Web End-User Quarantine (EUQ) permet aux utilisateurs finaux de :

- Créer un nouveau compte
- Configurer les actions de spam de la quarantaine et une liste d'expéditeurs approuvés
- Modifier les mots de passe

Les utilisateurs peuvent accéder à Hosted Email Security Web EUQ à l'URL suivant :

Europe, Moyen-Orient et Afrique :

http://emailsec-euq.trendmicro.eu

États-Unis et régions autres que Europe, Moyen-Orient et Afrique :

https://us.emailsec-euq.trendmicro.com

Vous trouverez plus d'informations sur Hosted Email Security Web EUQ à la section *Présentation de Web EUQ* à la page C-1, dans l'aide en ligne Web EUQ ou dans le *Guide de l'utilisateur final Hosted Email Security Web EUQ*.

Réinitialisation du mot de passe de l'utilisateur final

Les administrateurs système de messagerie peuvent indiquer aux utilisateurs finaux qui ont perdu leur mot de passe qu'ils peuvent utiliser le lien « Vous avez oublié votre mot de passe ? » dans la page Hosted Email Security Web EUQ afin de réinitialiser leur mot de passe. Pour pouvoir réinitialiser leur mot de passe, les utilisateurs finaux doivent répondre à la question de sécurité choisie lors de la création du compte.

Si les utilisateurs ne peuvent pas se souvenir de la question de sécurité, les administrateurs système de messagerie peuvent réinitialiser leur mot de passe. Lorsqu'un administrateur système de messagerie réinitialise le mot de passe de l'utilisateur final, il active automatiquement le compte. Un utilisateur final qui réinitialise le mot de passe reçoit presque immédiatement un e-mail d'authentification qui lui permet de se connecter à Web EUQ.

Journaux

La section Journaux vous permet de rechercher et de visualiser des journaux de suivi des messages en fonction d'une date spécifique ou d'une plage de dates, d'un expéditeur, d'une direction (entrante et sortante) ou d'un destinataire. Les informations de suivi des messages ne sont disponibles que pour les sept derniers jours.

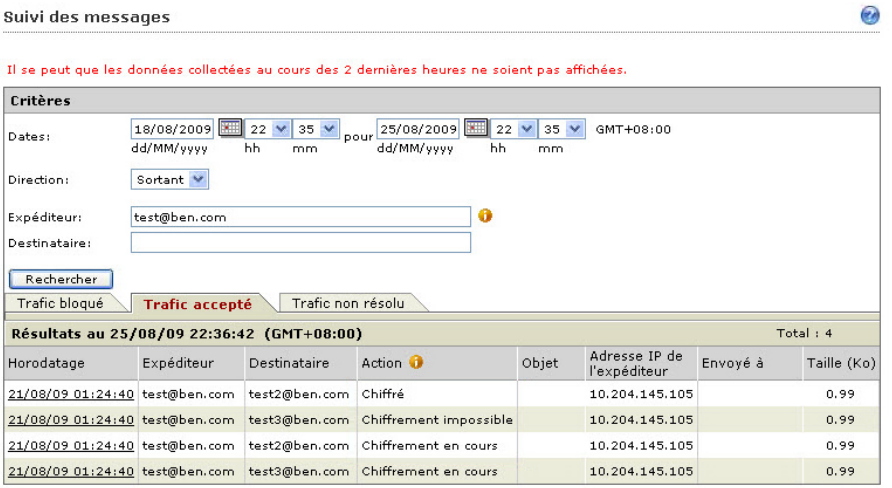


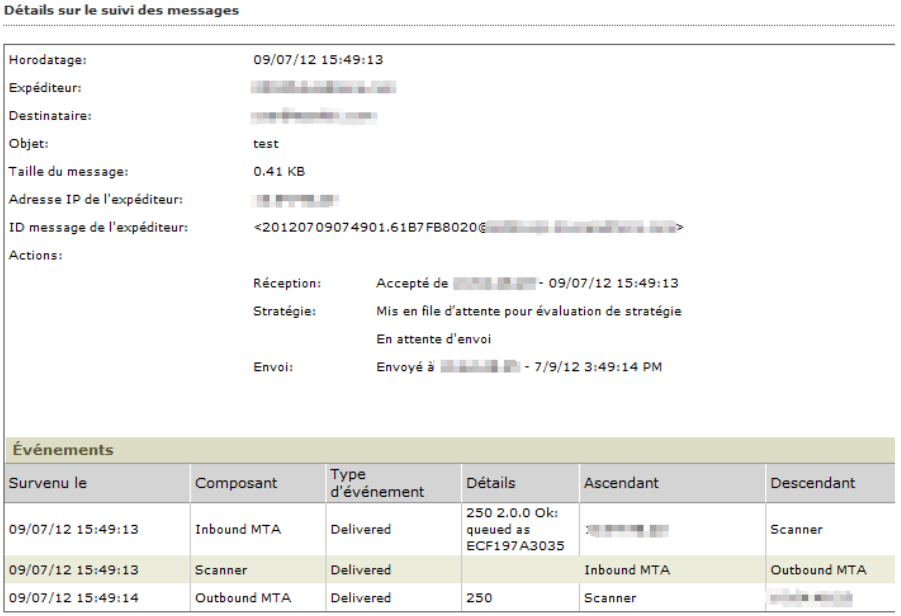
FIGURE 4-6. Écran Suivi des messages affichant les résultats d'une demande de trafic entrant

Détails sur le suivi des messages

Dans l'écran Suivi des messages, vous pouvez localiser les messages au sein du système en utilisant les informations sur l'expéditeur et/ou le destinataire. Les utilisateurs de Hosted Email Security peuvent rechercher des messages entrants et sortants. Un tableau de résultats indique l'état et l'action effectuée sur le message comme :

- Bloqué ou retardé à l'extérieur du système par le service de réputation (pour les messages entrants) ou par le service relais de messages Hosted Email Security (pour les messages sortants)
- Accepté pour traitement et supprimé avec un virus
- Accepté, traité et transmis
- Non résolu

Une recherche peut également être effectuée dans les e-mails envoyés via le protocole TLS (Transport Layer Security). Si l'icône TLS est affichée, ceci peut indiquer que Hosted Email Security a accepté/envoyé le trafic de messagerie de/à un ATM descendant via TLS.



Détails sur le suivi des messages

Horodatage:	09/07/12 15:49:13
Expéditeur:	[redacted]
Destinataire:	[redacted]
Objet:	test
Taille du message:	0.41 KB
Adresse IP de l'expéditeur:	[redacted]
ID message de l'expéditeur:	<20120709074901.61B7FB8020@[redacted]>
Actions:	
Réception:	Accepté de [redacted] - 09/07/12 15:49:13
Stratégie:	Mis en file d'attente pour évaluation de stratégie
	En attente d'envoi
Envoi:	Envoyé à [redacted] - 7/9/12 3:49:14 PM

Événements

Survenu le	Composant	Type d'événement	Détails	Ascendant	Descendant
09/07/12 15:49:13	Inbound MTA	Delivered	250 2.0.0 Ok: queued as ECF197A3035	[redacted]	Scanner
09/07/12 15:49:13	Scanner	Delivered		Inbound MTA	Outbound MTA
09/07/12 15:49:14	Outbound MTA	Delivered	250	Scanner	[redacted]

FIGURE 4-7. Détails des événements sur la page Détails du suivi des messages

Si vous cliquez sur l'horodatage d'une entrée de journal, l'écran Détails sur le suivi des messages s'affiche et fournit des informations supplémentaires sur ce message.

Les champs utilisés pour classifier chaque journal de suivi des messages sont décrits ci-dessous :

TABLEAU 4-2. Détails sur le suivi des messages

CHAMP	DESCRIPTION
Horodatage	Date et heure auxquelles le message a été accepté.
Expéditeur	Adresse électronique de l'expéditeur
Destinataire	Adresse électronique du destinataire. Pour les messages à destinataires multiples, seul le destinataire de cette copie du message est affiché.
objet.	Ligne d'objet du message (sauf horodatage).
Taille du message	Taille totale du message, pièces jointes incluses.
Adresse IP de l'expéditeur	Adresse IP du serveur source de l'expéditeur.
ID message de l'expéditeur	ID du message, comme indiqué dans le champ ID message : de l'en-tête de l'e-mail. Il s'agit normalement de l'ID de message créé par le client de messagerie de l'expéditeur sur lequel l'e-mail a été rédigé.
Actions	Actions effectuées par ce message. Elles sont regroupées en trois étapes : réception, stratégie et remise.

Événements	Cette section décrit le flux réel des messages. Les informations suivantes sont fournies : Survenu le : Horodatage réel du moment auquel est survenu le type d'événement. Composant : Le composant de messagerie ayant traité un événement. Type d'événement : Action finale pour ce processus spécifique. Les différents types d'événements sont les suivants : Envoyé, Retourné, Expiré, Supprimé, Mis en quarantaine, Redirigé, Envoyer maintenant, En attente d'envoi, Chiffrement en cours, Chiffré et Chiffrement impossible Détails : Description du flux du message. Ascendant/Descendant : La transmission d'un composant vers le suivant (ou d'une source vers la suivante).

Chapitre 5

Administration et réputation IP

Ce chapitre vous guide dans la configuration des paramètres de réputation IP et dans la réalisation de différentes tâches d'administration groupées dans le menu Administration.

Sujets abordés dans ce chapitre :

- *Paramètres de réputation IP* à la page 5-2
  - *Utilisation du curseur dynamique de réputation* à la page 5-3
  - *Réglage des paramètres d'exclusion IP* à la page 5-4
  - *Sélection des listes de réputation IP standard* à la page 5-5
  - *Listes de réputation IP Approuvés et Bloqués* à la page 5-7
  - *Dépannage des paramètres de réputation IP* à la page 5-10
- *Administration* à la page 5-11
  - *Modification des mots de passe* à la page 5-11
  - *Gestion des répertoires* à la page 5-13
  - *Vérification de votre répertoire d'utilisateurs* à la page 5-16
  - *Gestion des domaines* à la page 5-17
  - *Comarquage* à la page 5-22
  - *Services Web* à la page 5-29
  - *Afficher le contrat de niveau de service* à la page 5-31
  - *Gestion à distance* à la page 5-33
  - *Modes de licence* à la page 5-35

Paramètres de réputation IP

Hosted Email Security peut utiliser les fonctions de réputation IP de Trend Micro Email Reputation Services (ERS), service complémentaire proposé par Trend Micro. Vous pouvez accéder à ce service en cliquant sur **Réputation IP** dans le menu de gauche.

Vous pouvez utiliser le curseur dynamique de réputation pour régler le niveau de blocage des connexions e-mail par ERS. Vous pouvez également choisir le niveau de blocage des serveurs de messagerie à volume élevé, comme expliqué dans Réglage des paramètres d'exclusion *Réglage des paramètres d'exclusion IP* à la page 5-4.

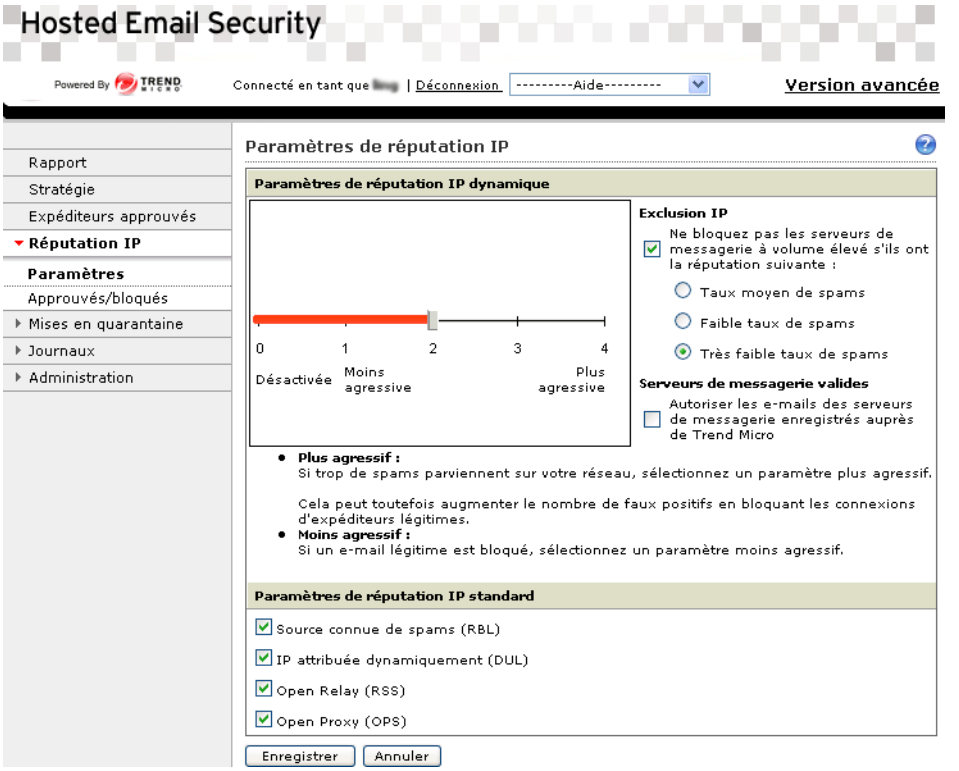


FIGURE 5-1. Écran Paramètres de réputation IP

Utilisation du curseur dynamique de réputation

Vous pouvez régler les niveaux de blocage à l'aide du curseur dynamique de réputation en procédant comme suit :

- **Plus restrictif** – Si trop de spams parviennent sur votre réseau, choisissez un paramétrage plus restrictif. Un tel paramétrage peut toutefois augmenter le nombre de faux positifs en bloquant les connexions d'expéditeurs légitimes.
- **Moins restrictif** – Si des e-mails légitimes se retrouvent bloqués, choisissez un paramétrage moins restrictif.

Conseil : Trend Micro recommande de modifier les paramètres dynamiques avec précaution et par petites étapes. Vous pouvez alors procéder à des réglages fins de vos paramètres en fonction de l'augmentation du nombre de spams et de messages légitimes reçus.

Pour régler les paramètres de réputation dynamique :

1. Dans le menu de gauche, sélectionnez **Réputation IP.** L'écran Paramètres de réputation IP s'affiche.
2. Réglez le curseur sur l'un des points suivants :

   Niveau 4 : paramétrage le plus restrictif. Si ERS (Email Reputation Services) détecte un seul message de spam reçu d'une adresse IP émettrice, il insère cette adresse dans la base de données de réputation dynamique. Le délai de stockage dans la base de données de l'adresse IP d'un émetteur dépend de la détection par ERS d'autres spams provenant de cet émetteur.

   Niveau 3 : paramétrage moyennement restrictif. ERS autorise une petite quantité de spams provenant d'émetteurs bien notés. Néanmoins, si ERS détecte une augmentation des spams supérieure au seuil autorisé pour cette catégorie d'émetteurs, il insère cet émetteur dans la base de données de réputation dynamique. Le délai de stockage dans la base de données de l'adresse IP d'un émetteur dépend de la détection par ERS d'autres spams provenant de cet émetteur. Ce délai peut être porté à une valeur maximale comme pour le niveau 4.

   Niveau 2 : paramétrage relativement peu restrictif. ERS autorise une quantité plus importante de spams provenant d'émetteurs bien notés. Néanmoins, si ERS détecte une augmentation des spams supérieure au seuil autorisé pour cette catégorie d'émetteurs, il insère cet émetteur dans la base de données de réputation dynamique. Le délai de stockage dans la base de données de l'adresse IP d'un émetteur est généralement plus court que pour le niveau 3.

Niveau 1 : paramétrage le moins restrictif. ERS autorise une quantité de spams provenant d'émetteurs bien notés identique à celle du niveau 2. Le délai de stockage dans la base de données de l'adresse IP d'un émetteur est en général plus court que pour le niveau 2.

Niveau 0 : interroge la base de données de réputation dynamique mais ne bloque aucune adresse IP.

3. Cliquez sur **Enregistrer**.

Remarque : Le niveau de blocage par défaut est le niveau 2 (paramétrage moyennement peu restrictif).

Réglage des paramètres d'exclusion IP

Les serveurs de messagerie à volume élevé peuvent émettre une quantité très importante d'e-mails, dont certains seront très probablement des spams. Ces serveurs, utilisés généralement par les grands FAI, peuvent envoyer une quantité suffisamment importante de spams pour qu'ERS (Email Reputation Services) place leur adresse IP sur une liste de blocage. Toutefois, vous souhaitez peut-être qu'ERS ne bloque pas ces serveurs, car trop de messages légitimes risqueraient d'être bloqués dans ce cas.

Outre le réglage du niveau de blocage des paramètres de réputation à l'aide du curseur, vous pouvez paramétrer ERS pour bloquer uniquement les serveurs de messagerie à volume élevé dont la réputation en matière de spam est moyenne, basse ou très basse.

Section d'exclusion IP

Les paramètres d'« exclusion IP » s'utilisent conjointement avec le curseur de réputation dynamique situé à gauche. Vous pouvez choisir de ne pas utiliser cette fonctionnalité en décochant la case **Ne pas bloquer les serveurs de messagerie à volume élevé (Tels que les FAI) s'ils ont la réputation suivante.**

Pour sélectionner un niveau d'exclusion pour les serveurs de messagerie à volume élevé :

1. Dans l'écran Paramètres de réputation IP, situé à droite de la section Paramètres de réputation dynamique, assurez-vous que la case **Ne pas bloquer les serveurs de messagerie à volume élevé s'ils ont une réputation de** reste cochée (valeur par défaut), puis choisissez l'une des options suivantes :
   - Taux de spams moyen
   - Taux de spams faible
   - Taux de spams très faible (valeur par défaut)
2. Cliquez sur **Enregistrer**. ERS exclura du blocage automatique tous les serveurs de messagerie à volume élevé qui correspondent à l'option choisie.

Serveurs de messagerie valides

Si vous cochez cette case, ERS autorisera les connexions à partir de tous les serveurs de messagerie désignés comme « serveurs de messagerie valides », qu'ils émettent ou non des spams. Cette liste est fondée sur les demandes clients des ATM de ces serveurs.

Sélection des listes de réputation IP standard

Vous pouvez sélectionner les listes à activer à partir de celles qui constituent la base de données standard de réputation des e-mails. Par défaut, toutes les listes sont activées. Ce paramétrage par défaut est la combinaison la plus efficace pour réduire les niveaux de spam, et elle répond aux besoins de la plupart des clients.

AVERTISSEMENT ! Si vous désactivez certaines parties de la base de données standard de réputation IP, vous pourrez constater une augmentation du nombre de spams qui parviennent sur votre serveur de messagerie interne en raison d'un filtrage supplémentaire de contenu.

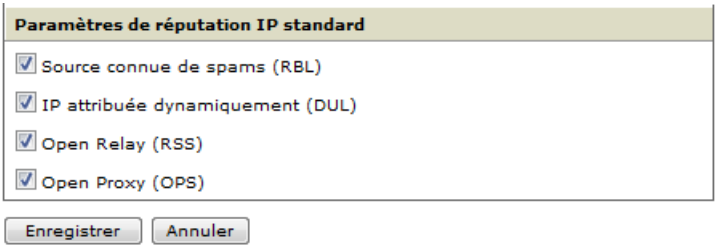


FIGURE 5-2. Par défaut, les quatre listes de réputation IP standard sont sélectionnées

La base de données standard de réputation IP comprend les quatre listes suivantes :

- **La liste des trous noirs en temps réel (RBL)** est une liste d'adresses IP de serveurs de messagerie connus pour être des sources de spam.
- **La liste dynamique des utilisateurs (DUL)** est une liste d'adresses IP attribuées dynamiquement, ou disposant de règles d'utilisation acceptables qui excluent les serveurs de messagerie publics. La plupart des éléments de cette liste sont gérés en coopération avec le FAI propriétaire de l'espace réseau. Les adresses IP de cette liste ne doivent pas envoyer directement des e-mails mais elles doivent utiliser les serveurs de messagerie de leur FAI.
- **La liste « Relay Spam Stopper » (RSS)** est une liste d'adresses IP de serveurs de messagerie utilisés comme des relais ouverts, connus pour avoir envoyé des spams. Un relais ouvert est un serveur qui accepte des e-mails de n'importe quel utilisateur d'Internet, rendant ainsi difficile ou impossible le suivi des spammeurs.
- **La liste « Open Proxy Stopper » (OPS)** est une liste d'adresses IP de serveurs de proxy ouverts, connus pour avoir envoyé des spams. Un serveur de proxy ouvert est un serveur qui accepte des connexions de n'importe quel utilisateur d'Internet et relaie les messages provenant de ces connexions sur n'importe quel serveur Internet, rendant ainsi difficile ou impossible le suivi des spammeurs.

Listes de réputation IP Approuvés et Bloqués

Les listes de réputation IP « Approuvés » et « Bloqués », comme le montre la *figure 5-4* à la page 5-9, permettent aux messages de pays, FAI, adresses IP ou plages CIDR approuvés de contourner le filtrage de niveau IP. Les listes Approuvés et Bloqués sont appliquées à votre compte Hosted Email Security, et non à votre ATM. Vous pouvez cependant configurer d'autres listes d'expéditeurs bloqués ou effectuer un filtrage supplémentaire au niveau de votre ATM.

Le contournement du filtrage IP présente l'inconvénient de nécessiter des ressources supplémentaires pour traiter, filtrer et stocker de nombreux messages de spam qui auraient été normalement bloqués. Si vous utilisez les listes Approuvés et Bloqués, il se peut que vous constatiez des taux moins élevés de détection de spams.

Remarque : Les listes de réputation IP « Approuvés » ne sont pas liées à la liste générale « Expéditeurs approuvés » dans le premier niveau du menu de gauche. Cet écran concerne uniquement les vérifications de réputation IP ; dans l'écran Expéditeurs approuvés, vous pouvez définir des adresses électroniques ou des domaines approuvés afin que Hosted Email Security ne les scanne pas.

Bloquer tous les pays sauf

L'onglet Bloqués propose une fonction absente de l'onglet Approuvés ; vous pouvez choisir de « bloquer tous les pays sauf » une liste sélectionnée de pays, comme le montre la *figure 5-3*.

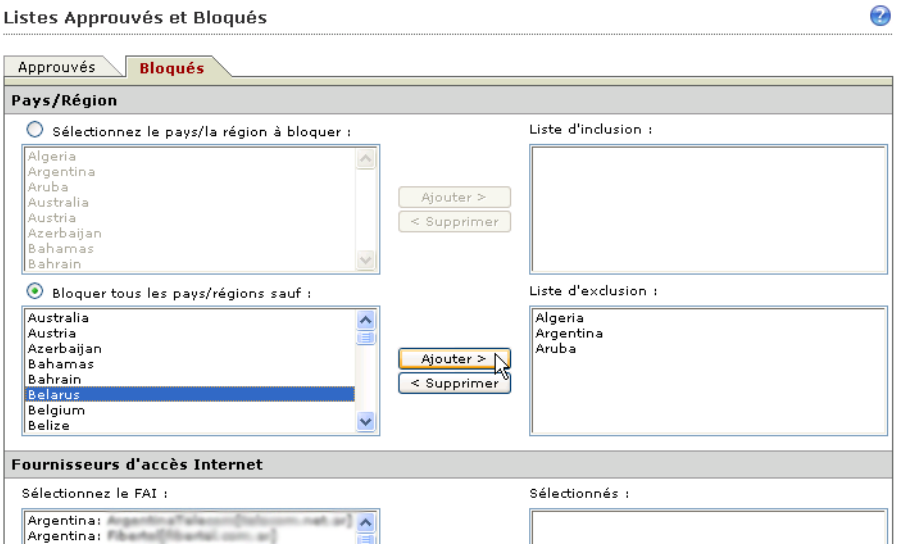


FIGURE 5-3. Écran Listes Approuvés et Bloqués : Fonction Bloquer tous les pays sauf

Cette fonction vous permet de configurer Hosted Email Security pour bloquer les e-mails de tous les pays sauf ceux figurant dans la liste des pays approuvés par votre entreprise.

En cas de recherche dans le service de réputation standard (RBL), l'ordre d'évaluation hiérarchique est le suivant :

1. IP approuvé
2. IP bloqué
3. FAI ou ASN approuvé
4. FAI ou ASN bloqué
5. Pays approuvé
6. Pays bloqué

Pour une recherche dans le service de réputation dynamique (QIL), les « listes de stratégies bloquées » définies par le client (IP, ISP/ASN, Pays) sont ignorées ; seules les listes Approuvés sont vérifiées. Sinon, l'ordre de recherche de stratégies (IP, FAI/ASN, Pays) est identique à celui du service de réputation standard (RBL).

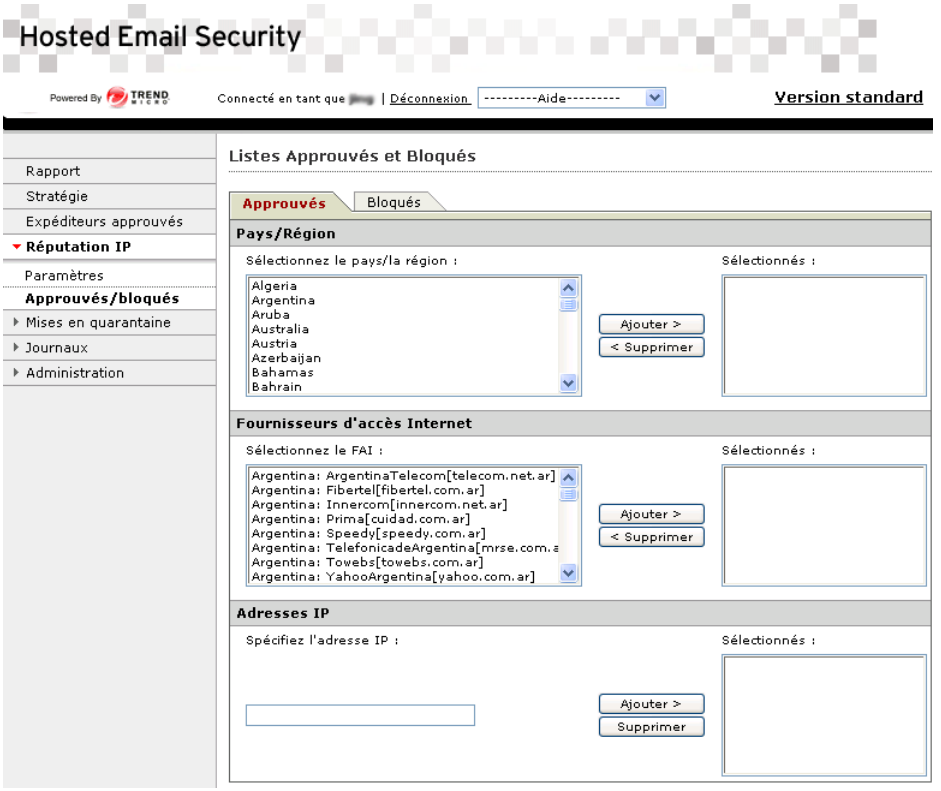


FIGURE 5-4. Écran Listes de réputation IP Approuvés et Bloqués

Dépannage des paramètres de réputation IP

Si vous rencontrez des erreurs inattendues lors de l'utilisation de l'écran Réputation IP, vous pourrez peut-être résoudre le problème par vous-même. Avant de contacter le support technique, consultez le *tableau 5-1* ci-dessous pour des conseils sur la résolution du problème.

TABLEAU 5-1. Guide de dépannage de l'écran Paramètres de réputation IP

PROBLÈME	CAUSE POSSIBLE	SOLUTION POSSIBLE
LE BOUTON ENREGISTRER EST DÉSACTIVÉ.	Je n'ai pas de code d'activation (AC).	Obtenez un code d'activation valide de votre fournisseur.
	J'ai demandé un code d'activation, mais il n'a pas encore été ajouté au système Hosted Email Security.	Réessayez dans une heure ou deux.
	Un problème réseau temporaire empêche Hosted Email Security de valider le code d'activation.	Réessayez dans quelques minutes.
JE NE PEUX PAS ENREGISTRER MES PARAMÈTRES DE RÉPUTATION IP.	Il y a un problème temporaire sur le réseau.	• Réessayez dans quelques minutes. • Déconnectez-vous, reconnectez-vous et réessayez.
	J'ai ouvert plusieurs fenêtres de navigateur dans l'écran Réputation IP du site Hosted Email Security et la session dans la fenêtre ouverte en premier a expiré.	Basculez vers la fenêtre ouverte dernièrement et fermez les autres fenêtres.

Administration

Dans la section Administration, vous trouverez des liens vers des écrans relatifs aux sujets suivants :

- *Modification du mot de passe administrateur* à la page 5-12
- *Réinitialisation d'un mot de passe pour Web EUQ* à la page 5-13
- *Gestion des répertoires* à la page 5-13
- *Gestion des domaines* à la page 5-17
- *Comarquage* à la page 5-22
- *Services Web* à la page 5-29
- *Afficher le contrat de niveau de service* à la page 5-31
- *Gestion à distance* à la page 5-33

Modification des mots de passe

Les administrateurs peuvent modifier le mot de passe administrateur, mais aussi réinitialiser un mot de passe oublié pour un utilisateur final qui doit accéder au service Hosted Email Security Web End User Quarantine (EUQ).

Tous les mots de passe Hosted Email Security requièrent entre 8 et 32 caractères. Trend Micro recommande vivement d'utiliser des mots de passe contenant des types de caractères multiples (mélange de lettres, chiffres et autres caractères) sous un format non reconnaissable (par exemple, n'utilisez pas votre date de naissance, plaque d'immatriculation, etc.).

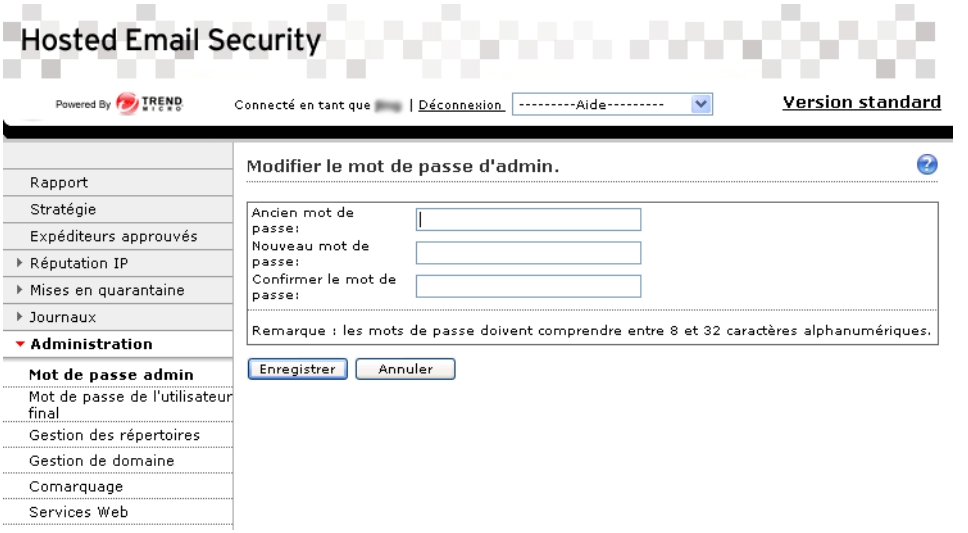


FIGURE 5-5. Écran Modification du mot de passe administrateur.

Modification du mot de passe administrateur

Pour modifier le mot de passe administrateur :

1. Accédez à **Administration > Mot de passe administrateur**.
2. Entrez votre mot de passe actuel/précédent
3. Entrez votre nouveau mot de passe.
4. Confirmez votre nouveau mot de passe.
5. Cliquez sur **Enregistrer**.

Réinitialisation d'un mot de passe pour Web EUQ

Les administrateurs système peuvent réinitialiser un mot de passe oublié par l'utilisateur final.

Pour réinitialiser un mot de passe de l'utilisateur final :

1. Cliquez sur **Administration > Mot de passe de l'utilisateur final.**

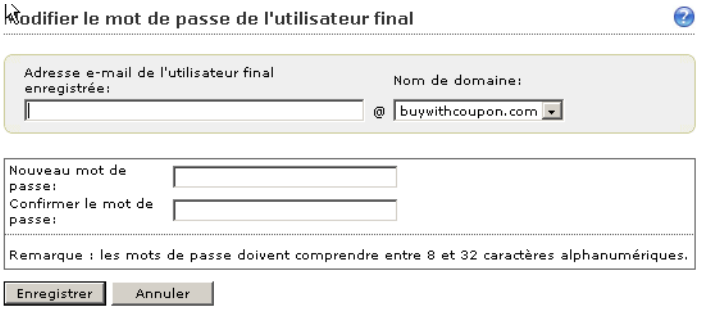

Modifier le mot de passe de l'utilisateur final
Adresse e-mail de l'utilisateur final enregistrée:
Nom de domaine:
@
buywithcoupon.com
Nouveau mot de passe:
Confirmer le mot de passe:
Remarque : les mots de passe doivent comprendre entre 8 et 32 caractères alphanumériques.
Enregistrer
Annuler

FIGURE 5-6. Écran Modification du mot de passe de l'utilisateur final

2. Saisissez l'adresse électronique de l'utilisateur final.
3. Saisissez et confirmez le nouveau mot de passe.

Remarque : L'utilisateur final devra connaître le nouveau mot de passe pour se connecter.

---

4. L'utilisateur final recevra un e-mail avec un URL d'activation.

   L'utilisateur final devra cliquer sur l'URL d'activation, puis saisir l'adresse électronique adéquate et le nouveau mot de passe dans l'écran de connexion à Hosted Email Security Web EUQ.

Gestion des répertoires

Hosted Email Security utilise des répertoires d'utilisateurs pour éviter la diffusion de spams, ainsi que les attaques de type DHA (Directory Harvest Attacks). Vous pouvez importer des répertoires d'utilisateurs pour permettre à Hosted Email Security de connaître les adresses électroniques et domaines légitimes de votre entreprise. Hosted Email Security ne reconnaît que les fichiers ANSI au format LDAP Data Interchange Format (LDIF : .ldf) et les valeurs séparées par des virgules au format ANSI ou UTF-8 (CSV : fichiers .csv).

L'écran Gestion des répertoires (Administration > Gestions des répertoires) comprend les éléments suivants :

- **Section Importer répertoire d'utilisateurs :** champs permettant d'importer un nouveau fichier de répertoire d'utilisateurs.
- **Répertoire d'utilisateurs importés :** désigne le ou les fichiers du répertoire d'utilisateurs actuellement utilisés par Hosted Email Security. Hosted Email Security remplace un seul utilisateur de domaine de messagerie à la fois. Les utilisateurs peuvent être une combinaison de répertoires d'utilisateurs multiples.

Remarques sur la gestion des répertoires

Avant d'importer un fichier de répertoire LDIF ou CSV, notez ce qui suit :

- Vous ne pouvez voir que les répertoires qui sont associés avec votre compte administrateur. Si vous partagez le service Hosted Email Security avec un autre administrateur, celui-ci ne verra pas les répertoires associés à ce compte lors de la connexion.
- Chaque fois que vous ajoutez des utilisateurs à votre réseau, vous devez importer vos répertoires d'utilisateurs mis à jour. Dans le cas contraire, Hosted Email Security rejette les messages électroniques de la part d'utilisateurs récemment ajoutés.
- N'ajoutez pas de lignes vides ou d'autres données inutiles au fichier que vous importez. Soyez attentif lors de la création d'un fichier.
- Chaque fois que vous importez un fichier de répertoire, l'ancien fichier de répertoire est écrasé.

  Cependant, si vous importez un fichier de répertoire d'utilisateurs mis à jour qui ne contient pas d'informations pour l'un de vos domaines, les entrées de ces domaines restent identiques pour Hosted Email Security et ne sont pas écrasées.

AVERTISSEMENT ! Soyez attentif lors de l'importation d'un répertoire. Si vous importez un fichier de répertoire mis à jour qui contient des informations pour l'un de vos domaines, toutes les entrées de ces domaines sont remplacées.

Exportation d'un fichier de répertoire d'utilisateurs

Exportez tout d'abord vos répertoires depuis votre système. Trend Micro recommande d'utiliser un outil LDIFDE pour créer un fichier LDIF. Pour des instructions sur l'utilisation de l'outil LDIFDE et la création du fichier, consultez le lien suivant sur le site Web de Microsoft : http://support.microsoft.com/kb/237677

Importation d'un fichier de répertoire d'utilisateurs

AVERTISSEMENT ! Trend Micro recommande vivement de ne pas importer plus de 24 répertoires par jour. Dans le cas contraire, votre système pourrait saturer.

Pour importer un fichier de répertoire d'utilisateurs :

1. Cliquez sur **Administration > Gestion des répertoires**. L'écran Gestion des répertoires s'affiche.

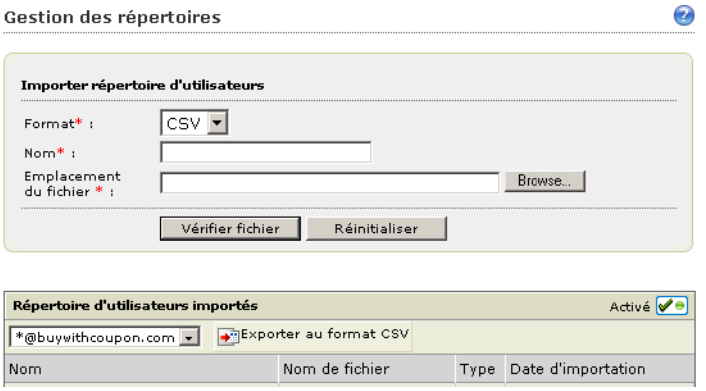


FIGURE 5-7. Écran Gestion des répertoires

2. Dans la liste déroulante **Format**, sélectionnez le type de format :
   - **LDIF**
   - **CSV**
3. Dans le champ **Nom**, tapez un nom descriptif pour le fichier.
4. Dans le champ **Emplacement du fichier**, saisissez le chemin du répertoire de fichiers et le nom de fichier ou cliquez sur **Parcourir** et sélectionnez le fichier .ldf ou .csv sur votre ordinateur.

5. Cliquez sur **Vérifier fichier**. Une fois que la barre de progression indique la fin du processus, un écran de résumé s'affiche et indique les éléments suivants :
   - **Résumé :** Récapitulatif des informations ci-dessus.
   - **Domaines et nombre d'utilisateurs devant remplacer les utilisateurs actuels :** les domaines que vous avez spécifiés lorsque vous avez souscrit au service Hosted Email Security.
   - **Domaines non valides :** les domaines compris dans votre fichier de répertoire, mais qui ne sont pas officiellement enregistrés dans votre service Hosted Email Security. Hosted Email Security ne peut fournir de services pour ces domaines et pour leurs adresses électroniques correspondantes.
6. Cliquez sur **Importer**.

Vérification de votre répertoire d'utilisateurs

Si vous n'êtes pas certain de connaître les domaines actifs des répertoires d'utilisateurs pour votre service, vous pouvez temporairement désactiver les répertoires, importer les fichiers, exporter les répertoires dans un fichier CSV et les visualiser sans que le répertoire ne soit opérationnel. Lorsque vous savez que le répertoire d'utilisateurs est correct, vous pouvez le réactiver.

Remarque : Les répertoires dans le fichier sont activés par défaut. Lorsqu'ils sont activés, une marque verte apparaît dans le tableau **Répertoire d'utilisateurs importés** : . Lorsqu'ils sont désactivés, un X rouge apparaît : . Hosted Email Security peut prendre jusqu'à cinq (5) minutes pour activer ou désactiver les répertoires.

Pour vérifier des répertoires d'utilisateurs :

1. Désactivez les répertoires en cliquant sur l'icône « Activé » ( ). La case à cocher devient un X rouge « Désactivé » ( ) et le mot **Désactivé** apparaît.
2. Importez le fichier de répertoire (voir la section *Pour importer un fichier de répertoire d'utilisateurs :* à la page 5-15).
3. Sélectionnez les domaines à vérifier.
4. Cliquez sur **Exporter** et enregistrez le fichier de répertoire (au format CSV).
5. Ouvrez le fichier de répertoire dans une application pouvant lire les fichiers CSV.
6. Vérifiez que les informations de répertoire sont correctes.
7. Réactivez les répertoires en cliquant sur l'icône « Désactivé » ( ).

Gestion des domaines

Au lieu de fournir manuellement au service d'assistance technique Trend Micro Hosted Email Security les domaines de votre société, vous pouvez utiliser l'écran Gestion de domaine pour ajouter, modifier ou supprimer des domaines.

À propos de l'état du domaine

L'état des domaines gérés peut être l'un des suivants :

- Normal : le domaine remet correctement les messages.
- Suspendu : le domaine n'a pas remis de messages au cours des 30 derniers jours.

  Hosted Email Security modifie l'état en Normal lorsque l'une des conditions suivantes est remplie :

  - Les messages sont correctement envoyés au domaine enregistré.
  - L'adresse IP du relais de domaine a changé.

  En outre, vous pouvez reprendre manuellement les domaines suspendus (voir page 5-22).
- Horodaté (période de grâce) : le domaine n'a pas remis de messages au cours des 5 derniers mois.

  Lorsqu'un domaine passe à cet état (à savoir qu'il ne lui reste qu'un mois avant d'être désactivé), Hosted Email Security crée une stratégie globale pour les domaines dont l'état est SUSPENDU. Hosted Email Security applique un horodatage à chaque message envoyé à ce domaine pour rappeler que si aucune action n'est entreprise, le domaine sera désactivé. Si vous reprenez un domaine, l'horodatage est supprimé, ainsi que la stratégie globale correspondante.
- Désactivé : le domaine est suspendu pendant au moins six mois ; le trafic via le relais a été inexistant pendant les 30 derniers jours.

  Lorsqu'un domaine est désactivé, vous ne pouvez plus reprendre son service ni modifier son état.

  La désactivation permanente d'un serveur désactive le domaine et empêche tous les messages d'être acheminés par Hosted Email Security vers ce serveur. Hosted Email Security analyse les enregistrements MX et efface ceux qui pointent vers le service pour empêcher la création d'une boucle de messages.

Lorsqu'un serveur est désactivé, tous les enregistrements MX supplémentaires de ce domaine sont supprimés. Ceci permet d'empêcher la création d'une boucle de messages. Par conséquent, cette fonctionnalité supprime les statistiques inexactes concernant les domaines gérés et évite le déclenchement de stratégies incorrectes.

Ajout d'un domaine

Pour ajouter un domaine :

1. Sélectionnez **Administration > Gestion de domaine** pour ouvrir l'écran Gestion de domaine présenté dans la figure *figure 5-8* ci-dessous.

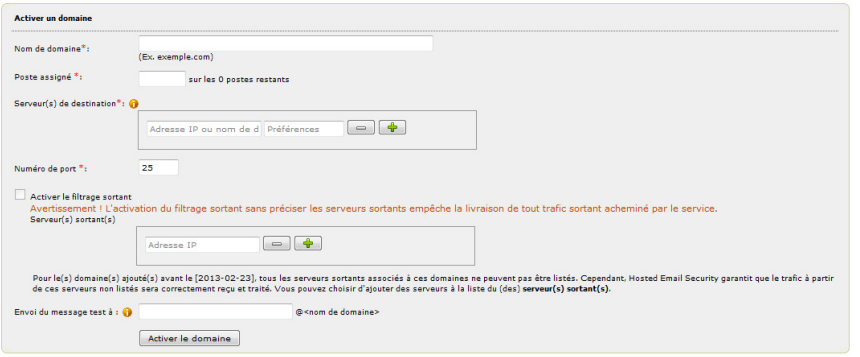

Activer un domaine
Nom de domaine*:
(Ex. exemple.com)
Poste assigné *:
sur les 0 postes restants
Serveur(s) de destination*:
Adresse IP ou nom de d
Préférences
Numéro de port *:
25
Activer le filtrage sortant
Avertissement ! L'activation du filtrage sortant sans préciser les serveurs sortants empêche la livraison de tout trafic sortant acheminé par le service.
Serveur(s) sortant(s)
Adresse IP
Pour le(s) domaine(s) ajouté(s) avant le [2013-02-23], tous les serveurs sortants associés à ces domaines ne peuvent pas être listés. Cependant, Hosted Email Security garantit que le trafic à partir de ces serveurs non listés sera correctement reçu et traité. Vous pouvez choisir d'ajouter des serveurs à la liste du (des) serveur(s) sortant(s).
Envoi du message test à :
@<nom de domaine>
Activer le domaine

FIGURE 5-8. Écran Gestion de domaine de Trend Micro Hosted Email Security, tel que vous le voyez lorsque vous vous connectez à l'aide d'un compte OLR

2. Saisissez les informations suivantes dans les champs prévus à cet effet (les champs obligatoires sont affichés en gras) :
   - Le nouveau **nom de domaine**
   - Le nombre de **postes assignés** à ce domaine

     L'intitulé «postes» correspond au nombre réel d'utilisateurs dans le domaine.
   - **Adresse IP/nom de domaine complet** (fully qualified domain name, FQDN) et numéro de préférence du serveur de destination

     Vous pouvez spécifier jusqu'à 30 serveurs de destination pour le trafic entrant. En outre, la valeur de préférence peut être comprise entre 1 et 100.

     Remarque : S'il existe plusieurs serveurs de destination vers un domaine de destinataire, l'ATM sélectionnera le serveur de destination avec le numéro de préférence minimum. Par conséquent, s'il existe deux serveurs de destination ou plus avec le même numéro de préférence, l'ATM doit choisir aléatoirement l'un d'eux comme ATM descendant.
   - **Numéro de port** du serveur de messagerie de destination
   - Adresse électronique test

     Utilisez cette adresse électronique comme destinataire d'un message test pour confirmer l'envoi par Hosted Email Security.
3. Sélectionnez **Activer le filtrage sortant**, puis indiquez l'adresse IP du (des) serveur(s) sortant(s). Vous pouvez spécifier jusqu'à 30 adresses IP de relais.
4. Cliquez sur **Activer le domaine.**

Si le domaine est valide et qu'il existe un enregistrement MX (initial et non modifié) pour celui-ci, le nouveau domaine, l'adresse IP ou le nom de domaine complet, le numéro de port, les postes assignés et d'autres informations s'affichent dans le tableau Domaines en bas de l'écran et Hosted Email Security envoie un message électronique de confirmation à l'adresse d'administration enregistrée.

Remarque : L'e-mail de confirmation envoyé par Hosted Email Security vous indique si l'ajout du domaine a réussi. Le processus d'ajout du domaine peut nécessiter 24 à 48 heures.

Pour ajouter immédiatement le domaine à la liste de domaines :

1. Attendez de recevoir l'e-mail de confirmation de Hosted Email Security.

   AVERTISSEMENT ! Ne modifiez pas votre enregistrement MX tant que vous n'avez pas reçu cet e-mail de confirmation.

2. Ajoutez le domaine à votre enregistrement MX.
3. Sélectionnez **Administration > Gestion de domaine** pour ouvrir l'écran Gestion de domaine.
4. Sélectionnez le domaine ajouté dans la liste de domaines. Son état est Vérification.
5. Cliquez sur **Vérifier enregistrement MX** pour vérifier que l'enregistrement MX du domaine a désigné l'ATM entrant de Hosted Email Security.

   Remarque : Si un nouveau domaine ne s'active pas et continue à afficher l'état Vérification, vérifiez l'enregistrement MX du domaine. Vérifiez que l'enregistrement MX pointe vers le nom de domaine complet Hosted Email Security correct.

Confirmation de l'envoi des messages par le service

Lors de l'ajout d'un domaine à Hosted Email Security, assurez-vous de bien saisir une adresse de messagerie test, comme mentionné dans l'*Étape 2* de la section *Ajout d'un domaine*. Après l'ajout du domaine et avant la redirection de votre enregistrement MX, envoyez un message test au compte de messagerie que vous avez entré et confirmez que les messages circulent librement via Hosted Email Security. Si vous ne recevez pas le message test, contactez votre fournisseur de service.

AVERTISSEMENT ! Ne modifiez pas votre enregistrement MX tant que vous n'avez pas reçu cet e-mail de confirmation.

Modification d'un domaine

Vous pouvez modifier les informations relatives au domaine dans l'écran **Gestion de domaine > {votre-domaine}**. Pour y accéder, cliquez sur le nom du domaine dans le tableau Domaines en bas de l'écran. Pour plus d'informations sur cet écran, consultez la *figure 5-9*.

Pour modifier un domaine :

1. Sélectionnez **Administration > Gestion de domaine** dans le menu de gauche pour ouvrir l'écran Gestion de domaine, comme l'indique la *figure 5-8*.
2. Cliquez sur le nom du domaine dans le tableau en bas de l'écran Gestion de domaine. L'écran **Gestion de domaine > {nom-de-votre-domaine}** s'affiche. Ses champs sont pré-renseignés avec les informations enregistrées pour ce domaine.
3. Effectuez les modifications nécessaires, puis cliquez sur **Enregistrer.**

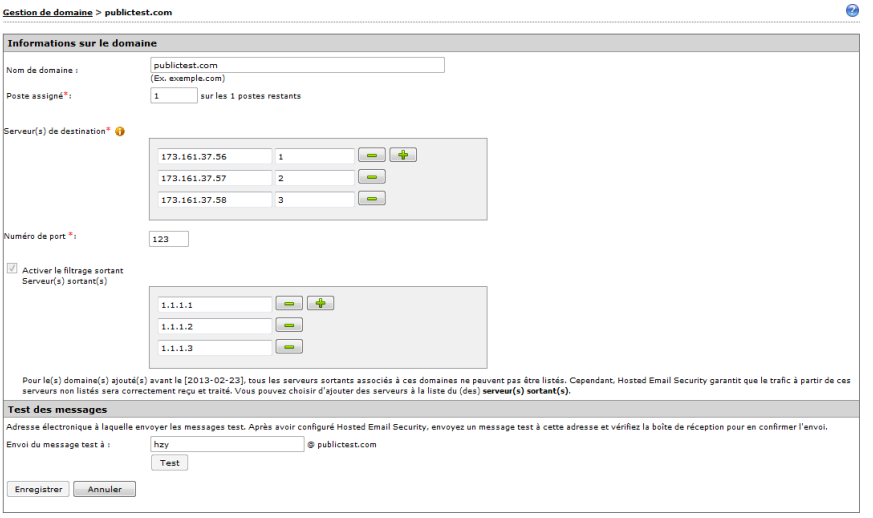

Gestion de domaine > publictest.com
Informations sur le domaine
Nom de domaine :
publictest.com
(Ex. exemple.com)
Poste assigné* :
1
sur les 1 postes restants
Serveur(s) de destination*
173.161.37.56
1
173.161.37.57
2
173.161.37.58
3
Numéro de port* :
123
Activer le filtrage sortant
Serveur(s) sortant(s)
1.1.1.1
1.1.1.2
1.1.1.3
Pour le(s) domaine(s) ajouté(s) avant le [2013-02-23], tous les serveurs sortants associés à ces domaines ne peuvent pas être listés. Cependant, Hosted Email Security garantit que le trafic à partir de ces serveurs non listés sera correctement reçu et traité. Vous pouvez choisir d'ajouter des serveurs à la liste du (des) serveur(s) sortant(s).
Test des messages
Adresse électronique à laquelle envoyer les messages test. Après avoir configuré Hosted Email Security, envoyez un message test à cette adresse et vérifiez la boîte de réception pour en confirmer l'envoi.
Envoi du message test à :
hzy
@ publictest.com
Test
Enregistrer
Annuler

FIGURE 5-9. Modification des informations relatives au domaine dans l'écran Gestion de domaine > {votre domaine} (modifiable uniquement si vous êtes connecté sur votre compte OLR)

Vous pouvez également désactiver un domaine depuis l'écran Gestion de domaine.

Pour désactiver un domaine :

1. Sélectionnez **Administration > Gestion de domaine** dans le menu de gauche pour ouvrir l'écran Gestion de domaine, comme l'indique la *figure 5-8*.
2. Cochez la case correspondant au domaine à désactiver.
3. Cliquez sur le lien **Désactiver** situé dans l'en-tête ou le pied de page du tableau. Votre demande de désactivation est transmise à Trend Micro pour être traitée.

Reprendre les domaines suspendus

Utilisez l'écran Gestion de domaine pour empêcher la désactivation des domaines suspendus.

Pour reprendre un domaine suspendu :

1. Sélectionnez **Administration** > **Gestion de domaine** dans le menu de gauche pour ouvrir l'écran Gestion de domaine.

   Sinon, après vous être connecté, cliquez sur le lien Suspendu qui vous redirigera vers l'écran Gestion de domaine.
2. Cochez la case correspondant au domaine à reprendre.
3. Cliquez sur le lien **Reprendre** situé dans l'en-tête ou le pied de page du tableau. Votre demande de désactivation est transmise à Trend Micro pour être traitée.

Comarquage

Hosted Email Security vous permet d'afficher le logo de votre entreprise dans la bannière supérieure et dans la page de connexion.

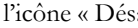
En tant que revendeur, vous pouvez comarquer la console d'administration Hosted Email Security, l'interface Web EUQ ou les deux. Vous pouvez définir différents domaines ayant des logos identiques ou différents, ou permettre aux administrateurs de domaine de définir le logo à afficher pour leur domaine. Vous pouvez également désactiver cette fonction.

Spécifications du logo

Avant de tenter d'établir un site en comarquage, vérifiez que l'image de votre logo répond aux impératifs suivants :

- **Hauteur :** Exactement 60 pixels (ni plus grande, ni plus petite)
- **Largeur :** 800 à 1680 pixels
- **Format de fichier :** .gif, .jpg ou .png

Comarquage de la console d'administration

1. Cliquez sur **Administration > Comarquage.** L'écran Comarquage s'affiche, comme le montre la *figure 5-10*.
2. Cliquez sur l'icône « Désactivé » (

) située dans le coin supérieur droit pour activer la fonction. L'icône change de forme pour indiquer que la fonction est « activée » (

).

Remarque : Le comarquage est désactivé par défaut.

FIGURE 5-10. Écran Comarquage

3. Dans la liste déroulante **Compte/domaine géré**, sélectionnez les comptes qui afficheront le logo, comme le montre la *figure 5-11* ci-dessous.

Powered By TREND MICRO
Connecté en tant que adminA
| Déconnexion
Pour la console d'administration, définissez le comarquage par nom de compte d'administration et non par nom de domaine.
omarquage
omaine/compte géré : adminA
ogo de bannière
adminA
*@example.com

FIGURE 5-11. Comarquage de la console d'administration (sélectionnez le nom de compte, et non le nom de domaine)

4. Cliquez sur **Parcourir** et accédez à l'emplacement de votre fichier de logo. (Pour supprimer le logo, cliquez sur **Effacer.)**.
5. Cliquez sur **Ouvrir** : un aperçu du logo s'affiche comme indiqué sur la *figure 5-12*.

FIGURE 5-12. Affichage du logo du domaine à configurer

6. Cliquez sur **Enregistrer**. L'image du logo s'affiche dans la bannière supérieure de la console d'administration Hosted Email Security (voir *figure 5-14*) et dans la page de connexion lorsque vous y accédez, comme l'explique la section *Accès à un site comarqué* à la page 5-27.

Comarquage de l'interface Web EUQ

En tant que revendeur, vous pouvez comarquer l'interface Web EUQ. La procédure est pratiquement identique à celle permettant d'établir une version en comarquage de la console d'administration Hosted Email Security, à une exception près, exposée ci-dessous.

Pour configurer une version en comarquage de Web EUQ :

1. Cliquez sur **Administration > Comarquage.** L'écran Comarquage s'affiche, comme le montre la *figure 5-10*.
2. Cliquez sur l'icône « Désactivé » (

) située dans le coin supérieur droit pour activer la fonction. L'icône change de forme pour indiquer que la fonction est activée (

).

Remarque : Le comarquage est désactivé par défaut.

---

3. Dans la liste déroulante **Compte/domaine géré**, sélectionnez le nom de domaine pour lequel le logo s'affichera, comme le montre la *figure 5-13* ci-dessous.

FIGURE 5-13. Comarquage de Web EUQ (sélectionnez le nom de domaine, et non le nom de compte)

4. Cliquez sur **Parcourir** et accédez à l'emplacement du fichier de logo (Pour supprimer le logo, cliquez sur **Effacer**.).
5. Cliquez sur **Ouvrir** : un aperçu du logo s'affiche comme indiqué sur la *figure 5-12*.
6. Cliquez sur **Enregistrer**. L'image du logo s'affiche dans la bannière supérieure de la console d'administration Hosted Email Security Web EUQ et dans l'écran de connexion EUQ (voir *figure 5-15*) lorsque vous y accédez, comme l'explique la section *Accès à un site comarqué* à la page 5-27.

Remarque : Les revendeurs peuvent définir différents logos pour différents domaines ou autoriser les administrateurs système du domaine à définir le logo du domaine en question, indépendamment du logo du revendeur. Le logo sélectionné pour un nom de compte s'affichera uniquement dans la console d'administration Hosted Email Security. Le logo sélectionné pour un domaine s'affichera uniquement dans la barre supérieure de l'interface Hosted Email Security Web EUQ associée au domaine en question.

The ABCD Company
Powered By TREND MICRO
TREND MICRO
Hosted Email Security
Saisissez votre nom d'utilisateur et votre mot de passe pour accéder à la console d'administration.
Connectez-vous avec le nom d'utilisateur et le mot de passe d'enregistrement en ligne Trend Micro. Qu'est-ce que c'est
Nom d'utilisateur :
adminA@example.com
Mot de passe :
Vous avez oublié votre mot de passe ?
Connexion

FIGURE 5-14. Échantillon d'un logo revendeur configuré dans la barre supérieure de l'écran de connexion Hosted Email Security

The ABCD Company
Powered By TREND MICRO
TREND MICRO
Hosted Email Security
Saisissez votre adresse électronique et votre mot de passe pour accéder à la console de services.
Adresse électronique :
user@example.com
Mot de passe :
Vous avez oublié votre mot de passe ?
Enregistrer un nouveau compte
Connexion

FIGURE 5-15. Le logo du domaine s'affiche dans la barre supérieure de l'écran de connexion de Hosted Email Security Web EUQ

Accès à un site comarqué

En tant que revendeur, vous pouvez fournir à vos clients une URL pour accéder au site comarqué.

Accès à une console d'administration comarquée

Vous avez différentes options pour accéder à une console d'administration comarquée, en fonction de votre type de connexion. Si vous avez enregistré votre compte à partir du site Web d'enregistrement en ligne (OLR) de Trend Micro, ajoutez le nom de compte OLR Hosted Email Security et associez votre marque à l'URL de base.

Par exemple, en supposant que le nom du compte OLR Hosted Email Security soit adminA, tapez ce qui suit dans la barre d'adresses du navigateur :

« https://us.emailsec.trendmicro.com/**adminA/co-brand** »

Si vous n'avez pas enregistré votre compte à partir du site Web OLR, vous pouvez vous connecter comme précédemment, en ajoutant le nom de compte Hosted Email Security d'origine à l'URL de base, comme suit :

« https://us.emailsec.trendmicro.com/**adminA** »

Accès à un site Web EUQ comarqué

Pour accéder à un site Web EUQ comarqué, les utilisateurs finaux ajoutent le nom de domaine à l'URL de base :

« https://us.emailsec-euq.trendmicro.com »

Par exemple, si le nom de domaine est « example.com », les utilisateurs finaux doivent entrer ce qui suit dans la barre d'adresses de leur navigateur :

« https://us.emailsec-euq.trendmicro.com/**example.com** »

Remarque : Si un utilisateur final accède à un site comarqué sans ajouter le nom de compte ou le nom de domaine, ce site s'affichera et sera fonctionnel, mais ne présentera pas l'apparence comarquée.

Services Web

Hosted Email Security vous permet d'accéder aux applications de services Web Hosted Email Security via un client de service Web Hosted Email Security installé dans votre environnement.

Vous devez suivre trois étapes avant de pouvoir accéder aux applications de services Web Hosted Email Security. Premièrement, vous avez besoin d'une clé d'authentification de service. Cette clé est l'identifiant global unique qui permet à votre client de services Web de s'authentifier et d'accéder aux services Web Hosted Email Security. Deuxièmement, vous devez activer les services Web Hosted Email Security. Troisièmement, vous devez sélectionner et installer le programme client de service Web sur votre environnement.

Pour préparer votre environnement de services Web :

1. Cliquez sur **Administration** > **Services Web**.

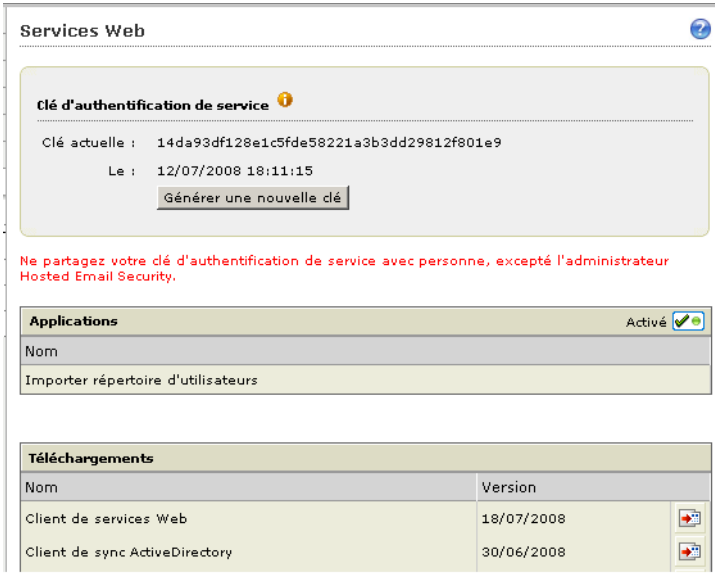
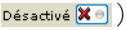


FIGURE 5-16. Écran Services Web

2. Assurez-vous de disposer d'une clé d'authentification de service. La clé actuelle affiche la clé que le programme client des services Web doit utiliser. Si vous générez une nouvelle clé, vous devez mettre à jour le programme client pour utiliser cette clé. La clé d'authentification de service est semblable à un mot de passe permettant au client de communiquer avec les services Web Hosted Email Security. Merci de divulguer cette clé uniquement aux administrateurs Hosted Email Security autorisés.

   Remarque : Si le champ **Clé actuelle** est vierge, cliquez sur **Générer une nouvelle clé** pour générer une nouvelle clé d'authentification de service.

3. Cliquez sur l'icône « Désactivé » () située dans le coin droit pour activer la fonction ( ).

   Elle est désactivée par défaut.

4. Dans la liste **Téléchargements**, sélectionnez le programme client des services Web Hosted Email Security à télécharger. Cliquez sur l'icône de téléchargement ( ) pour télécharger le client.
5. Enregistrez le client sur votre disque local.
6. Suivez les étapes d'installation pour installer le client.

Téléchargement du Guide des services Web Hosted Email Security

Trend Micro a préparé un guide destiné à vous aider à comprendre et utiliser le service Web. Vous pouvez télécharger le *Guide des services Web* dans la section Téléchargements de l'écran Services Web, comme le montre la *figure 5-17* à la page 5-31.

Conseil : Trend Micro vous recommande de télécharger et de vous familiariser avec le Guide des services Web avant de tenter d'effectuer une configuration avancée des services Web.

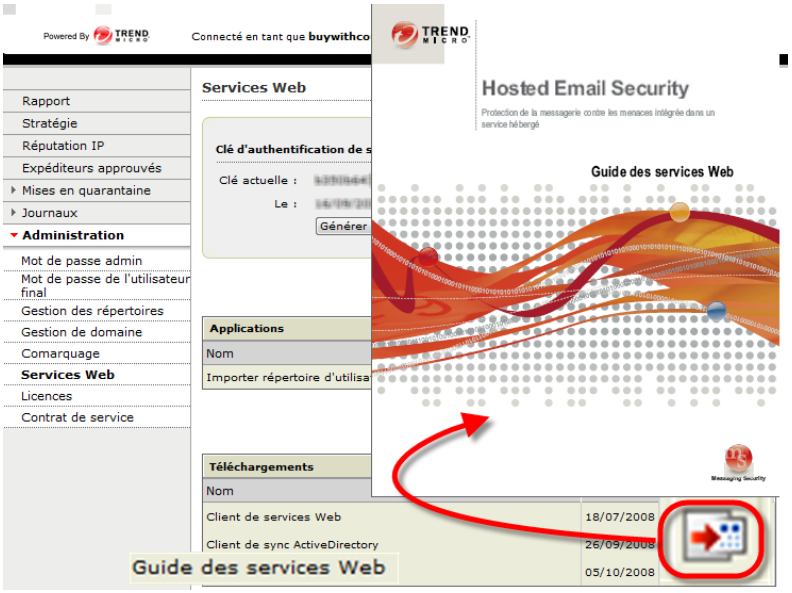


FIGURE 5-17. Téléchargez le Guide des services Web Hosted Email Security dans la section Téléchargements de l'écran Services Web

Afficher le contrat de niveau de service

Trend Micro propose un contrat de niveau de service offensif pour Hosted Email Security, qui permet à votre entreprise de bénéficier de la sécurité et de la permanence du service de messagerie pour une meilleure prise en charge de votre activité.

Ce contrat de niveau de service recouvre la disponibilité, le temps de latence, le blocage des spams, les faux positifs, la protection contre les virus et l'assistance. La dernière version de ce contrat, consultable ou téléchargeable à partir de l'écran Contrat de niveau de service Hosted Email Security, comporte des garanties correspondant à chaque niveau de service.

Remarque : Comme les dispositions de ce contrat varient en fonction des zones géographiques, assurez-vous de choisir la langue et la zone géographique appropriées lorsque vous utilisez cet écran.

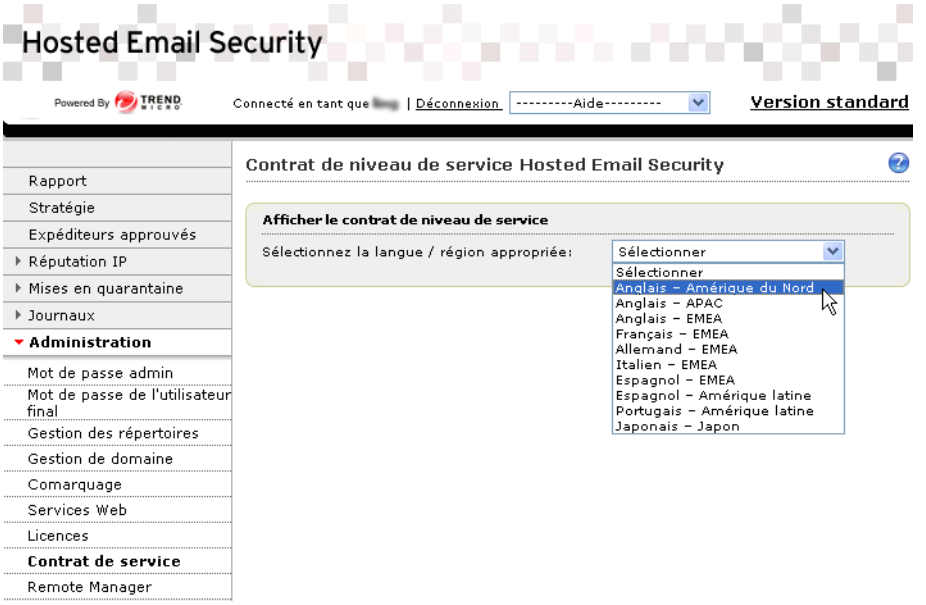


FIGURE 5-18. Écran du contrat de niveau de service Hosted Email Security

Pour afficher le contrat de niveau de service de votre zone géographique :

1. Dans le menu de gauche, sélectionnez **Administration > Contrat de service**. Le contrat de niveau de service Hosted Email Security s'affiche comme indiqué dans la *figure 5-18*.

   Conseil : Désactivez tous les bloqueurs de fenêtres intempestives de votre navigateur pour pouvoir télécharger le contrat de niveau de service.

2. Dans la liste déroulante, sélectionnez votre **langue/zone géographique.** Hosted Email Security ouvre une nouvelle fenêtre du navigateur et affiche (au format PDF d'Adobe Reader) le contrat de niveau de service correspondant à votre zone géographique dans la langue sélectionnée.

Remarque : Trend Micro se réserve le droit de modifier ce service à tout moment et sans préavis. La version actuelle du contrat de niveau de service Hosted Email Security est consultable par les clients enregistrés et les clients qui utilisent une version d'évaluation.

Gestion à distance

Vous pouvez utiliser l'écran Délégation de la gestion du compte, comme le montre la *figure 5-19*, pour désigner temporairement une personne chargée de gérer les stratégies de votre compte Hosted Email Security. Cette fonctionnalité peut être utile pour les revendeurs, qui gèrent souvent les comptes de plusieurs clients Hosted Email Security. Une personne chargée de la gestion Hosted Email Security peut consulter et modifier les stratégies et les paramètres Hosted Email Security à l'aide d'un produit Trend Micro distinct, Trend Micro Worry-Free Remote Manager (WFRM).

La console WFRM propose un récapitulatif des paramètres Hosted Email Security. Pour gérer Hosted Email Security depuis WFRM, le revendeur clique sur un lien dans WFRM qui ouvre la fenêtre Hosted Email Security. Cette fenêtre permet au revendeur d'apporter aux stratégies toutes les modifications qu'il est possible d'effectuer dans la console d'administration Hosted Email Security. (Pour plus d'informations sur ce produit, consultez le site Web Trend Micro.)

Pour désigner une personne, vous devez connaître sa clé d'autorisation du service. Vous pouvez obtenir cette clé auprès de votre revendeur, qui la génère depuis le produit WFRM.

FIGURE 5-19. Écran Gestion à distance (Délégation de la gestion du compte) sans délégation

Pour désigner une personne chargée de gérer un compte à distance :

1. Dans le menu de gauche, cliquez sur **Administration > Remote Manager**. L'écran Délégation de la gestion du compte s'affiche, comme l'indique la *figure 5-19* ci-dessus.
2. Tapez ou collez la clé d'autorisation du service de la personne chargée de gérer le compte et cliquez sur **Connecter.** Si la connexion aboutit, l'écran est rechargé et affiche le nom du compte et le délégué, l'adresse postale de cette personne, son adresse électronique et son numéro de téléphone portable, la clé du contrat et la date de début de délégation, comme le montre la *figure 5-20* à la page 5-34.

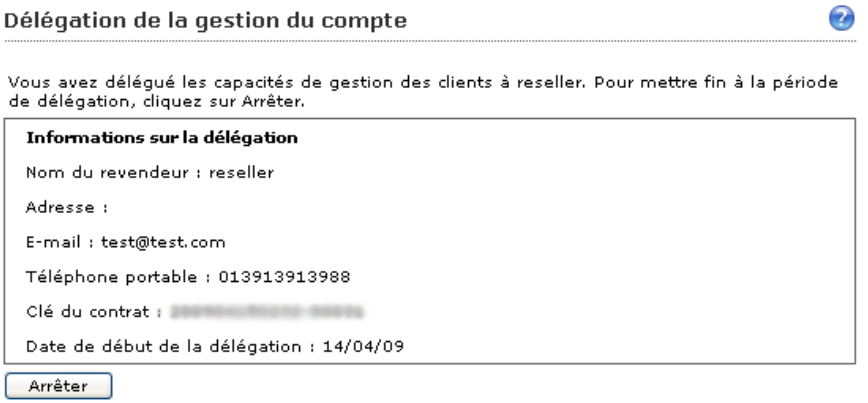

Délégation de la gestion du compte
Vous avez délégué les capacités de gestion des clients à reseller. Pour mettre fin à la période de délégation, cliquez sur Arrêter.
Informations sur la délégation
Nom du revendeur : reseller
Adresse :
E-mail : test@test.com
Téléphone portable : 013913913988
Clé du contrat :
Date de début de la délégation : 14/04/09
Arrêter

FIGURE 5-20. Gestion à distance : délégation de la gestion du compte

Vous pouvez mettre fin à tout moment à la délégation en cliquant sur **Arrêter** dans cet écran.

La personne chargée de la gestion du compte peut également mettre fin à la délégation depuis Worry Free Remote Manager. Lorsque cette personne effectue l'opération à distance, l'écran Délégation de la gestion du compte présente la plupart des informations affichées dans la version « déléguée » de l'écran (*figure 5-20*) ainsi que le motif de cet arrêt, comme l'indique la *figure 5-21* ci-après.

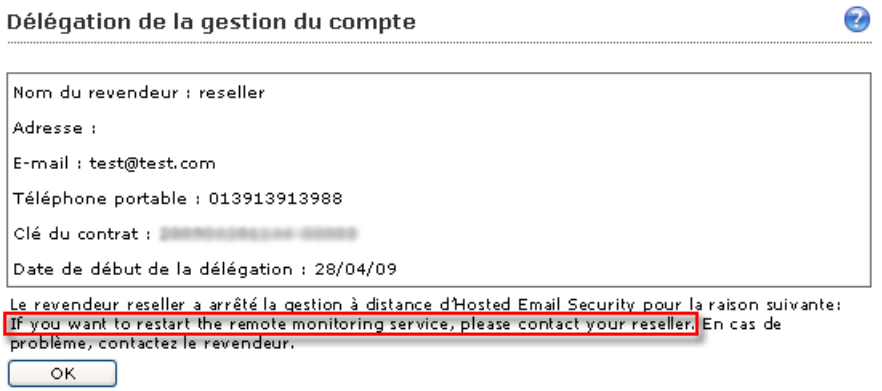

Délégation de la gestion du compte
Nom du revendeur : reseller
Adresse :
E-mail : test@test.com
Téléphone portable : 013913913988
Clé du contrat :
Date de début de la délégation : 28/04/09
Le revendeur reseller a arrêté la gestion à distance d'Hosted Email Security pour la raison suivante:
If you want to restart the remote monitoring service, please contact your reseller. En cas de problème, contactez le revendeur.
OK

FIGURE 5-21. Écran Délégation de la gestion du compte lorsque le délégué à distance a mis fin à la délégation

Modes de licence

Lorsque votre licence arrive à expiration, elle passe par différents modes avant d'être totalement désactivée. Pour comprendre les différents modes de licence, reportez-vous au tableau suivant.

TABLEAU 5-2. Modes de licence

MODE DE LICENCE	DESCRIPTION	DURÉE	ÉTAT DE PROTECTION	OPÉRATION POUVANT ÊTRE EFFECTUÉE
Active	La licence est valide.	En général une année, en fonction de l'abonnement	Les domaines sont protégés par le service.	Aucune ; vérifiez simplement la date d'expiration de votre licence.

TABLEAU 5-2. Modes de licence (Suite)

MODE DE LICENCE	DESCRIPTION	DURÉE	ÉTAT DE PROTECTION	OPÉRATION POUVANT ÊTRE EFFECTUÉE
Période de grâce	La licence est arrivée à expiration, mais elle est dans la période de grâce.	En général un mois, en fonction de l'abonnement	Les domaines sont protégés par le service. Une notification est envoyée au détenteur de la licence enregistrée.	Renouvelez votre licence immédiatement.
Expiration totale	La période de grâce est terminée et la licence est arrivée à expiration totale.	30 jours	• Le service continue à filtrer les messages, mais il ajoute une notification aux messages entrants. Les destinataires du message voient cette notification. • L'accès à la console d'administration est bloqué.	• Renouvelez votre licence immédiatement. • Contactez votre fournisseur de services d'assistance pour désactiver *temporairement* l'horodatage des messages entrants.
Désactivée	Toutes les données d'abonnement sont supprimées de manière permanente.	Permanente	• Toutes les données du domaine, de la stratégie et de la messagerie sont supprimées. • Tous les messages entrants sont rejetés (*code de réponse 554*).	Procurez-vous une nouvelle licence.

Annexe A

Foire Aux Questions

La FAQ suivante s'applique à la version actuelle de Hosted Email Security.

Question 1 : Qu'est-ce que Trend Micro™ Hosted Email Security ?
Réponse : Trend Micro Hosted Email Security est un service hébergé de sécurité de messagerie, profitable aux entreprises de toute taille. Nous fournissons le matériel, le logiciel et l'expertise en matière de messagerie pour protéger vos messages du spam, des virus, des vers, des chevaux de Troie et des attaques de phishing (vol d'identité). Le flux de messages nettoyés est directement envoyé à votre serveur de messagerie pour une remise finale à vos utilisateurs finaux.

Question 2 : Quels sont les avantages d'un service hébergé de sécurité de messagerie ?
Réponse : En tant que service hébergé hors site, Hosted Email Security peut arrêter les attaques avant qu'elles n'atteignent votre réseau. En plus d'arrêter le spam, les virus, les vers, les chevaux de Troie et autres programmes malveillants, Hosted Email Security peut protéger votre réseau des attaques qui :

- Tentent de bloquer votre connexion Internet (refus de service)
- Volent vos adresses électroniques pour les spammeurs (attaques DHA - Directory Harvest Attacks)

Question 3 : Ai-je besoin d'acheter/de mettre à niveau du matériel ou des logiciels ?

Réponse : Hosted Email Security est un service hébergé. Vous n'avez pas besoin d'acheter de matériel, ni de logiciel supplémentaire. Le service est géré par des professionnels de la sécurité, pour décharger votre équipe informatique des tâches d'installation, de maintenance et de réglage d'un système de sécurité de messagerie complexe.

Question 4 : Combien coûte le service ?

Réponse : Le prix de Trend Micro Hosted Email Security est fixé par utilisateur et par an. Le coût par utilisateur baisse lorsque le nombre d'utilisateurs augmente. Trend Micro ne facture aucun forfait de configuration, ni de frais d'assistance supplémentaire. Bien que cela soit improbable, votre société d'hébergement Web peut vous facturer des frais minimes pour changer d'enregistrement MX. Contactez votre service d'hébergement Web pour connaître les politiques de tarification.

Question 5 : Quel est le niveau de confidentialité de ce service ? (Je ne veux pas que quelqu'un consulte mes e-mails.)

Réponse : Tous les messages sont traités automatiquement et en toute transparence. Bon nombre de messages sont rejetés avant même d'être reçus, en fonction de la réputation de l'IP qui tente de les envoyer. Les messages reçus sont traités à travers un système de filtrage de spam et de virus multicouches, sans intervention humaine. Les messages ne sont jamais stockés, sauf si le serveur de messagerie est indisponible.

Question 6 : Pourquoi devrais-je faire confiance à Trend Micro pour la gestion de ma messagerie ?

Réponse : Trend Micro est un leader reconnu dans la gestion des menaces. L'entreprise bénéficie de plus de 10 ans d'expérience dans la messagerie et la prévention du spam, et de plus de 25 ans dans l'offre de solutions leader en matière d'antivirus. Trend Micro se positionne comme numéro 1 sur le marché des fournisseurs de solutions de passerelle Internet depuis six ans, et comme numéro 1 du marché des antivirus pour serveurs de messagerie depuis 4 ans. Nous connaissons et nous comprenons les problèmes générés par la sécurisation des réseaux contre tous les types de menaces, qu'elles proviennent ou non des e-mails. Une passerelle de messagerie sécurisée est l'un des composants d'une solution complète de sécurité réseau.

Question 7 : De quoi ai-je besoin pour utiliser ce service ?
Réponse : Pour utiliser ce service, vous avez uniquement besoin d'une passerelle Internet ou d'une connexion de messagerie de groupe de travail existante et d'un navigateur Web pour accéder aux rapports en ligne et à la console d'administration.

Question 8 : Comment commencer à utiliser ce service ? (Ai-je besoin d'installer, de configurer ou d'administrer quoi que ce soit ?)
Réponse : Une simple redirection de votre enregistrement Mail eXchange (MX) suffit pour démarrer le service. Vos e-mails sont traités par Trend Micro Hosted Email Security qui supprime les spams, les virus, les vers, les chevaux de Troie et les attaques de phishing ; les messages nettoyés sont ensuite directement envoyés à votre serveur de messagerie.

Question 9 : Comment rediriger mes e-mails/mon enregistrement Mail eXchange ?
Réponse : Si vous gérez votre propre DNS, vous pourrez facilement rediriger votre enregistrement MX. Si votre DNS est géré par un tiers ou un fournisseur d'accès Internet (FAI), celui-ci pourra le faire pour vous ou vous fournir une interface Web vous permettant de le faire vous-même. Vous pourrez attendre jusqu'à 48 heures pour que les modifications soient appliquées au système.

Pour connaître le nom de domaine complet correct de Hosted Email Security, consultez la base de connaissances Trend Micro à l'adresse suivante :

http://esupport.trendmicro.com

Question 10 : Comment accepter les messages provenant du service ?
Réponse : Pour vérifier que vous pouvez recevoir les messages traités par le service :

- Configurez votre pare-feu pour qu'il accepte le trafic issu des adresses IP Hosted Email Security
- Configurez votre serveur de messagerie pour qu'il accepte les transactions issues de ces adresses IP

Les adresses IP Hosted Email Security peuvent être modifiées. Pour obtenir la liste complète des adresses, consultez la base de connaissances Trend Micro à l'adresse :

http://esupport.trendmicro.com/Pages/How-to-accept-emails-coming-from-Hosted-Email-Security-servers-only.aspx

Question 11 : Pourquoi mon domaine garde-t-il l'état Vérification ?
Réponse : Lorsque vous activez un nouveau domaine, Hosted Email Security effectue quelques vérifications et vous envoie un message de confirmation. Dès que vous recevez ce message, vous devez modifier l'enregistrement MX du domaine pour pointer vers le nom de domaine complet correct de Hosted Email Security. Si vous ne mettez pas à jour l'enregistrement MX du domaine, le domaine garde l'état Vérification.

Pour plus d'informations, veuillez consulter *Gestion des domaines* à la page 5-17.

Question 12 : Puis-je essayer le service sur un nombre limité d'utilisateurs ?
Réponse : Nous vous recommandons d'utiliser un domaine test pour évaluer le service. Vous pourrez ainsi tester ses fonctionnalités pour différents types d'utilisateurs.

Question 13 : La remise de mes e-mails va-t-elle être retardée par l'utilisation de ce service ?
Réponse : Le temps nécessaire pour traiter chaque message se mesure en millisecondes. Tout retard de remise de vos messages est donc négligeable et à peine perceptible par l'utilisateur final.

Question 14 : Trend Micro stocke-t-il/archive-t-il les e-mails ?
Réponse : Hosted Email Security ne stocke pas et n'archive pas les e-mails par défaut. Tous les messages sont traités et immédiatement transmis à travers l'ATM du client. Les messages ne sont ni mis en file d'attente, ni stockés en mémoire, sauf si votre serveur de messagerie est indisponible. Toutefois, si vous créez une stratégie pour mettre les messages en quarantaine (les spams, par exemple), ces messages seront stockés dans notre centre de données pendant 21 jours au maximum dans la région EMEA et pendant 15 jours dans toutes les autres régions.

Question 15 : Comment réinitialiser ou renvoyer un mot de passe d'utilisateur final pour Web EUQ ?
(Un ou plusieurs utilisateurs ont perdu leur mot de passe ou ne s'en souviennent plus.)
Réponse : Cliquez sur **Administration** > **Mot de passe de l'utilisateur final** et remplissez le formulaire Modification du mot de passe de l'utilisateur final. L'utilisateur final recevra un e-mail avec une URL d'activation et devra cliquer sur celle-ci puis entrer l'adresse électronique appropriée et un nouveau mot de passe dans l'écran Hosted Email Security Web EUQ. Pour plus d'informations, veuillez consulter *Réinitialisation d'un mot de passe pour Web EUQ* à la page 5-13.

Question 16 : Qu'arrive-t-il à mes messages si mon serveur de messagerie est indisponible pendant un certain temps ? (Proposez-vous des solutions dans le cadre d'une récupération après sinistre ?)

Réponse : Si votre serveur de messagerie est indisponible pour une raison ou une autre, votre flux de messages est automatiquement mis en file d'attente pendant cinq jours au maximum ou jusqu'à ce que le serveur redevienne disponible. Vous ne perdrez donc pas d'e-mails importants à cause d'une défaillance matérielle ou logicielle, d'une panne d'alimentation, d'une défaillance réseau ou d'une erreur humaine.

Question 17 : Où est acheminé mon courrier sortant ?

Réponse : Par défaut, votre flux de messages sortants est directement géré par votre propre serveur de messagerie et transmis aux autres réseaux de la même façon. Cependant, avec une version complète, vous pouvez opter pour la redirection de vos messages sortants par le biais des services Hosted Email Security.

Si vous disposez d'un compte d'enregistrement en ligne (OLR) Trend Micro, vous pouvez désormais activer facilement le filtrage sortant, comme l'explique la section *Si vous disposez d'un compte d'enregistrement en ligne* à la page 2-7.

Si vous ne disposez pas d'un compte OLR, consultez les instructions de la section *Si vous ne disposez pas d'un compte d'enregistrement en ligne* à la page 2-7.

Question 18 : Les revendeurs et les clients finaux peuvent-ils se connecter à l'aide des informations de connexion existantes ?

Réponse : Oui. Il n'y a aucun changement pour les revendeurs et clients finaux xSP. Les revendeurs xSP peuvent toujours utiliser le rôle « au nom de » pour gérer leurs clients finaux. Les revendeurs et clients finaux xSP ne peuvent pas utiliser l'écran Gestion de domaine pour gérer leurs domaines. Ils peuvent utiliser la ligne de commande pour effectuer cette opération comme auparavant.

Question 19 : Comment puis-je modifier un nom de domaine géré ?

Réponse : Dans l'écran Gestion de domaine, vous pouvez modifier manuellement les informations de domaine à l'exception du nom de domaine. Pour modifier un nom de domaine, vous devez désactiver le domaine existant, puis ajouter le nouveau nom de domaine.

Question 20 : Comment puis-je utiliser la fonctionnalité de message test ?
Réponse : La fonctionnalité de message test permet de vérifier le bon fonctionnement du système Hosted Email Security. Si vous n'avez pas reçu de message pendant un certain temps, vous pouvez vérifier le fonctionnement de Hosted Email Security en envoyant un message test. Si le message test vous parvient, Hosted Email Security fonctionne correctement. Si vous ne recevez pas le message, contactez votre fournisseur de services d'assistance.

Question 21 : Pourquoi l'écran Gestion de domaine est-il désactivé ?
Réponse : Ce problème peut survenir si vous vous connectez à l'aide d'un compte local. Après la création de votre compte d'enregistrement en ligne (OLR) Trend Micro, vous pouvez encore vous connecter à Hosted Email Security à l'aide de vos informations de connexion antérieures pendant un certain temps. Toutefois, lorsque vous êtes connecté avec votre ancien compte, vous ne pouvez effectuer aucune modification dans l'écran Gestion de domaine.

Pour ajouter un nouveau domaine ou gérer un domaine existant :

1. Accédez à l'écran de connexion du service Trend Micro Hosted Email Security.
2. Sélectionnez **Se connecter avec un nom d'utilisateur et un mot de passe d'enregistrement en ligne Trend Micro**.
3. Entrez les nom d'utilisateur et mot de passe de votre compte OLR.
4. Cliquez sur **Connexion**. L'écran Rapports s'affiche.
5. Ajoutez ou gérez le domaine conformément aux instructions de la rubrique *Gestion des domaines* à la page 5-17.

Question 22 : Que se passe-t-il lorsque ma licence arrive à expiration ?
Réponse : Immédiatement après son expiration, votre licence passe par une période de grâce pendant laquelle le fonctionnement du service reste identique. Après cette période de grâce, une notification est ajoutée aux messages entrants et vous n'avez plus accès à la console d'administration. Vos données sont supprimées de manière permanente. Pour éviter toute interruption inopinée de votre service de messagerie, renouvelez votre licence avant son expiration.

Pour plus d'informations sur les modes de licence et sur la validité de votre licence, consultez la section *Modes de licence* à la page 5-35.

Annexe B

Informations de contact et ressources Internet

Cette annexe fournit des informations sur la manière d'obtenir une aide complémentaire pour vos questions d'assistance technique.

Sujets abordés dans cette annexe :

- *Contacter l'assistance technique* à la page B-2
- *Centre d'informations de sécurité* à la page B-7
- *Disponibilité du service* à la page B-3
- *Soumission de code suspect à Trend Micro* à la page B-4
- *TrendLabs* à la page B-7

Contacter l’assistance technique

Outre l’aide en ligne de Hosted Email Security, accessible dans la console d’administration, Trend Micro propose une assistance technique sur son site Web.

Trend Micro n’assure plus d’assistance technique par e-mail, mais offre une assistance via un système de soumission en ligne disponible à l’adresse :

http://fr.trendmicro.com/fr/products/enterprise/hosted-email-security/support/index.html

Sur le site mentionné ci-dessous, vous trouverez les informations de contact de l’assistance technique les plus récentes ainsi qu’un lien vers la base de connaissances Trend Micro.

Les clients disposant de comptes Hosted Email Security via Worry Free Business Security avec Hosted Email Security trouveront les informations de contact concernant ce produit sur le site ci-dessus.

Informations de contact générales

Numéro général de téléphone et de fax aux États-Unis :

Tél. : +1 (408) 257-1500 (principal)

Fax : +1 (408) 257-2003

Notre siège social américain est situé au cœur de la Silicon Valley :

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014, États-Unis

Disponibilité du service

Des temps d'arrêt planifiés pour cause de maintenance peuvent avoir lieu de temps en temps, avec une notification écrite préalable de 24 heures. Dans le cas d'un temps d'arrêt non planifié, une disponibilité de 99,99 % minimum est garantie à l'année.

Remise d'e-mails

La remise d'e-mails est garantie même si votre serveur de messagerie est temporairement indisponible. Le service continue de scanner et traiter les e-mails dans le cas d'une récupération après sinistre dans le sens descendant, alors que les e-mails valides sont stockés pendant cinq jours, selon le volume. Une fois que vos serveurs de messagerie locaux sont disponibles, les e-mails sont remis avec un contrôle intelligent du flux qui garantit une facilité de gestion dans le sens descendant, évitant ainsi toute saturation inutile des ressources en aval.

Base de connaissances

La base de connaissances de Trend Micro est une ressource en ligne disponible 24h/24 et 7j/7. Elle contient des milliers de procédures d'auto-assistance technique pour les produits Trend Micro. Utilisez la base de connaissances si vous obtenez, par exemple, un message d'erreur et que vous souhaitez connaître la procédure à suivre. De nouvelles solutions sont ajoutées tous les jours.

Vous trouverez également dans la base de données des foires aux questions sur les produits, des conseils avisés, des conseils pour se prémunir contre les virus, et les coordonnées locales des services d'assistance et de vente.

http://esupport.trendmicro.com/

Si vous ne trouvez pas la réponse que vous cherchez, la base de connaissances propose un service supplémentaire qui vous permet de soumettre votre question par e-mail. Le temps de réponse est généralement de 24 heures au maximum.

Soumission de code suspect à Trend Micro

Vous pouvez envoyer vos virus, fichiers infectés, chevaux de Troie, vers présumés, spyware et autres fichiers suspects à Trend Micro pour leur évaluation. Consultez pour cela l'URL de l'assistant de transmission « Trend Micro Submission Wizard » :

http://subwiz.trendmicro.com/SubWiz

Cliquez sur le lien **Submit a suspicious file/undetected virus** (Soumettre un fichier suspect/virus non détecté).

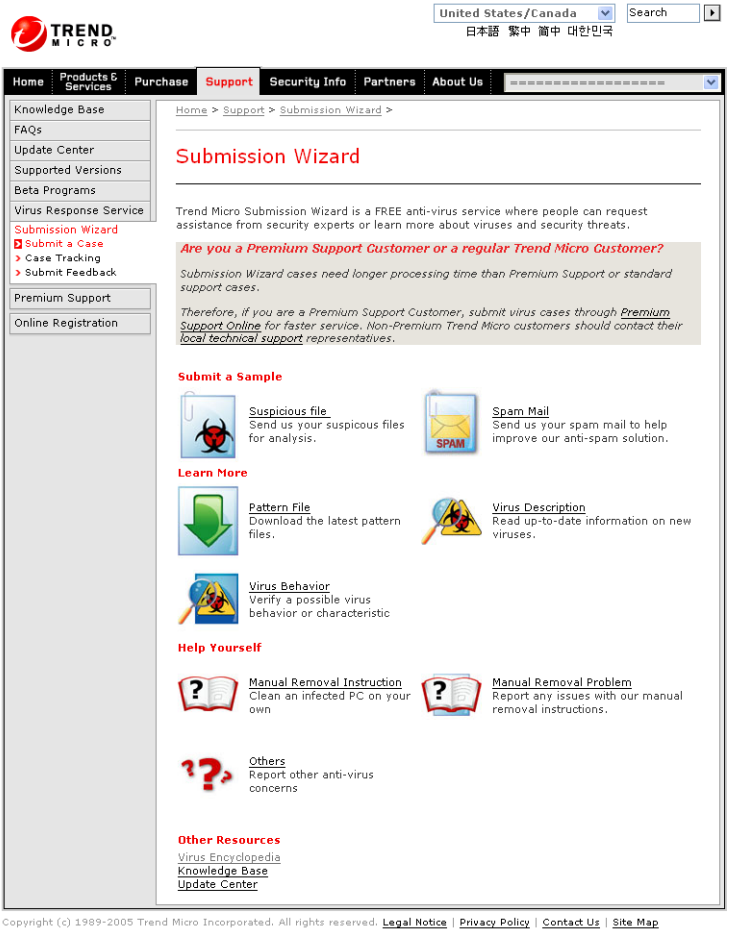

United States/Canada
Search
日本語 繁中 簡中 대한민국
Home
Products & Services
Purchase
Support
Security Info
Partners
About Us
Knowledge Base
FAQs
Update Center
Supported Versions
Beta Programs
Virus Response Service
Submission Wizard
Submit a Case
Case Tracking
Submit Feedback
Premium Support
Online Registration
Home > Support > Submission Wizard >
Submission Wizard
Trend Micro Submission Wizard is a FREE anti-virus service where people can request assistance from security experts or learn more about viruses and security threats.
Are you a Premium Support Customer or a regular Trend Micro Customer?
Submission Wizard cases need longer processing time than Premium Support or standard support cases.
Therefore, if you are a Premium Support Customer, submit virus cases through Premium Support Online for faster service. Non-Premium Trend Micro customers should contact their local technical support representatives.
Submit a Sample
Suspicious file
Send us your suspicous files for analysis.
Spam Mail
Send us your spam mail to help improve our anti-spam solution.
Learn More
Pattern File
Download the latest pattern files.
Virus Description
Read up-to-date information on new viruses.
Virus Behavior
Verify a possible virus behavior or characteristic
Help Yourself
Manual Removal Instruction
Clean an infected PC on your own
Manual Removal Problem
Report any issues with our manual removal instructions.
Others
Report other anti-virus concerns
Other Resources
Virus Encyclopedia
Knowledge Base
Update Center
Copyright (c) 1989-2005 Trend Micro Incorporated. All rights reserved. Legal Notice | Privacy Policy | Contact Us | Site Map

FIGURE B-22. Écran de l'assistant de transmission

Il vous est demandé de fournir les informations suivantes :

- **Email** (Messagerie électronique) : l'adresse électronique à laquelle vous voudriez recevoir la réponse de l'équipe antivirus.
- **Product** (Produit) : le produit ou le service que vous utilisez actuellement. Si vous utilisez plusieurs produits ou services Trend Micro, sélectionnez celui qui a le plus d'incidence sur le problème soumis, ou celui que vous utilisez le plus communément.
- **Number of Infected Seats** (Nombre de postes infectés) : le nombre d'utilisateurs infectés dans votre entreprise.
- **Upload File** (Télécharger fichier) : Trend Micro recommande de créer un fichier zip protégé par mot de passe avec le fichier suspect, en utilisant le mot « virus » comme mot de passe, puis de sélectionner le fichier zip protégé dans le champ **Upload File**.
- **Description** (Description) : veuillez inclure une brève description des symptômes. Notre équipe d'ingénieurs, spécialisée dans les virus, « dissèque » le fichier pour identifier et définir les risques qu'il pourrait contenir, et vous renvoie le fichier nettoyé généralement sous 48 heures.

Remarque : Les soumissions réalisées grâce à l'assistant de transmission/Virus Doctor sont traitées rapidement et ne font pas l'objet des politiques et limitations présentées dans l'Accord sur les niveaux de service « Trend Micro Virus Response Service Level Agreement ».

Lorsque vous cliquez sur **Next** (Suivant), un écran de remerciements s'affiche. Il indique également le numéro de suivi du problème soumis (Tracking Number).

Si vous préférez communiquer par message électronique, envoyez une requête à l'adresse suivante :

virusresponse@trendmicro.com

Aux États-Unis, vous pouvez aussi appeler ce numéro de téléphone gratuit :

(877) TRENDAV, ou 877-873-6328

TrendLabs

TrendLabs est l'infrastructure internationale de Trend Micro qui regroupe des centres régionaux de recherche antivirus et d'assistance. Ils fournissent aux clients des informations de sécurité actualisées en permanence.

Ces « Virus Doctors » de TrendLabs surveillent les risques de sécurité potentiels à travers le monde, pour s'assurer que les produits Trend Micro restent sécurisés contre les risques émergeants. La portée de ces efforts se mesure au jour le jour, alors que les mises à jour des fichiers de signatures de virus et les ajustements du moteur de scan fréquemment partagés avec les clients.

L'équipe de TrendLabs se compose de plusieurs centaines d'ingénieurs et de membres certifiés du personnel qui proposent un large éventail de services d'assistance technique et d'assistance produit. Les centres de services spécialisés et les équipes de réaction rapide sont situés à Tokyo, Manille, Taipei, Munich, Paris, et Lake Forest (Californie).

Centre d'informations de sécurité

Des informations de sécurité complètes sont disponibles gratuitement par Internet, sur le site Web de Trend Micro consacré aux informations de sécurité :

http://www.trendmicro.com/vinfo/fr/virusencyclo/default.asp

Visitez le site des informations de sécurité pour :

- Lire le rapport hebdomadaire sur les virus (Weekly Virus Report) qui répertorie les risques attendus pour la semaine en cours, et décrit, pour la même période, les 10 risques majeurs à l'échelle internationale.
- Consulter l'Encyclopédie des virus qui compile les risques connus avec une évaluation du risque, les symptômes d'infection, les plates-formes concernées, l'évolution des dommages, des instructions sur la suppression du risque, ainsi que des informations sur les canulars informatiques.
- Télécharger les fichiers de test d'EICAR (European Institute of Computer Anti-virus Research) afin de vous aider à tester la configuration de votre produit ou service de sécurité.
- Lire des informations générales sur les virus telles que :
    - Le Tour d'horizon des virus, qui vous aide à comprendre les différences entres les virus, les chevaux de Troie, les vers et autres risques.
    - Le *Guide de l'informatique sans risque* de Trend Micro.

- Il s'agit d'une description de l'évaluation des risques pour vous aider à comprendre leurs dommages potentiels. Le risque est évalué de la façon suivante : très bas, bas, moyen ou élevé.
- Un glossaire de la terminologie sur les virus et autres risques de sécurité.
- Des livres blancs complets du secteur à télécharger.

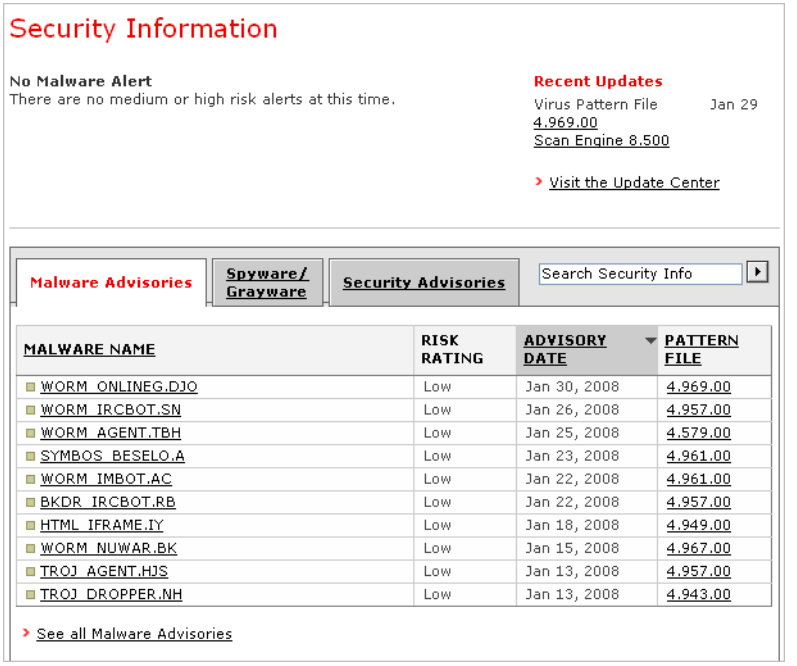

Security Information
No Malware Alert
There are no medium or high risk alerts at this time.
Recent Updates
Virus Pattern File
Jan 29
4.969.00
Scan Engine 8.500
Visit the Update Center
Malware Advisories
Spyware/ Grayware
Security Advisories
Search Security Info
MALWARE NAME
RISK RATING
ADVISORY DATE
PATTERN FILE
WORM_ONLINEG.DJO Low Jan 30, 2008 4.969.00
WORM_IRCBOT.SN Low Jan 26, 2008 4.957.00
WORM_AGENT.TBH Low Jan 25, 2008 4.579.00
SYMBOS_BESELO.A Low Jan 23, 2008 4.961.00
WORM_IMBOT.AC Low Jan 22, 2008 4.961.00
BKDR_IRCBOT.RB Low Jan 22, 2008 4.957.00
HTML_IFRAME.IY Low Jan 18, 2008 4.949.00
WORM_NUWAR.BK Low Jan 15, 2008 4.967.00
TROJ_AGENT.HJS Low Jan 13, 2008 4.957.00
TROJ_DROPPER.NH Low Jan 13, 2008 4.943.00
See all Malware Advisories

FIGURE B-23. Écran du site des informations de sécurité « Trend Micro Security Information »

- Souscrivez gratuitement au service d'alerte antivirus de Trend Micro pour en savoir plus sur les épidémies (en temps réel) et obtenir le rapport hebdomadaire sur les virus.
- En savoir plus sur les outils de mise à jour antivirus disponibles gratuitement pour les webmestres.

Annexe C

Présentation de Web EUQ

Cette annexe est destinée à vous aider à comprendre et utiliser Hosted Email Security Web End User Quarantine. Elle contient l'ensemble des informations du Guide d'utilisation de *Web End User Quarantine de Trend Micro*, que vous pouvez télécharger sous forme de manuel PDF séparé.

Hosted Email Security Web EUQ (End User Quarantine) est une interface utilisateur permettant aux utilisateurs finaux de gérer les spams mis en quarantaine. Elle permet également aux utilisateurs de configurer une liste d'expéditeurs approuvés dont les messages électroniques doivent arriver dans la boîte de réception et non être mis en quarantaine. Cette interface est facile d'utilisation, comme l'indique la *figure C-1*.

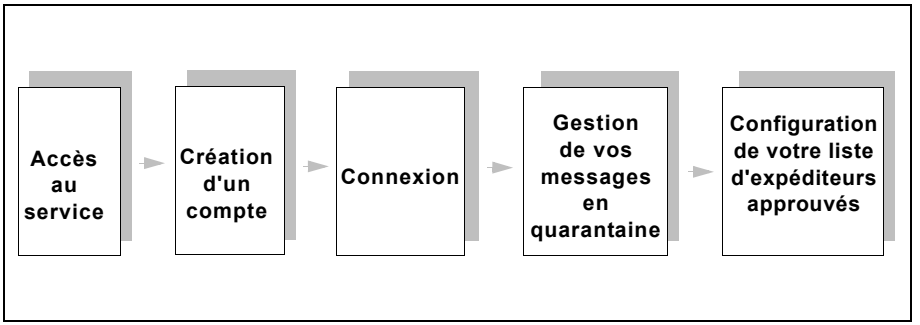


FIGURE C-1. Démarrage de Hosted Email Security Web EUQ

Accès au service Web End User Quarantine

L'accès au service Web End User Quarantine requiert une connexion Internet et l'un des navigateurs suivants :

- Microsoft™ Internet Explorer™, version minimale 6.0
- Mozilla™ Firefox™, version minimale 2.0

Pour accéder au service :

1. Ouvrez votre navigateur.
2. Accédez à l'URL fourni par votre administrateur système de votre messagerie.

Création d'un compte

Pour utiliser Web EUQ, vous devez créer un compte.

Pour enregistrer un nouveau compte :

1. Accédez au service.
2. Cliquez sur le lien **Enregistrer un nouveau compte** sur la page de connexion indiquée à la *figure C-2*.

Hosted Email Security
TREND MICRO
Hosted Email Security
Saisissez votre nom d'utilisateur et votre mot de passe pour accéder à la console d'administration.
Nom d'utilisateur :
Mot de passe :
Connexion
Vous avez oublié votre mot de passe ?

FIGURE C-2. Hosted Email Security Écran de connexion à Web EUQ

3. Entrez vos nom et prénom dans les champs de la zone Informations personnelles indiqués à la *figure C-3*.

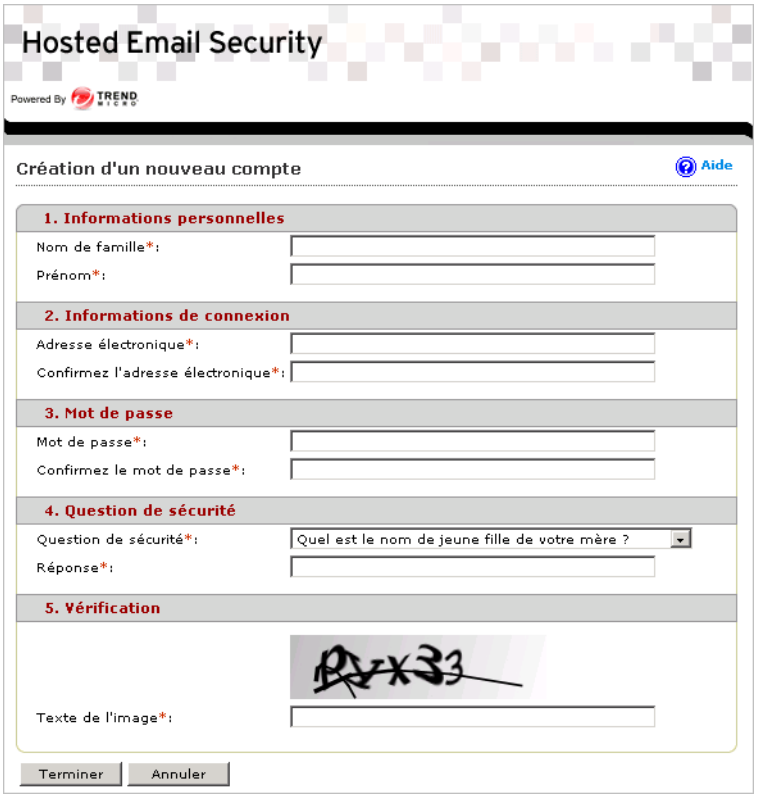


FIGURE C-3. Écran Création d'un nouveau compte

4. Entrez et confirmez votre adresse électronique dans les champs de la zone Informations de connexion.
5. Entrez deux fois le mot de passe associé au nouveau compte.
6. Sélectionnez une question de sécurité et entrez la réponse.
7. Entrez le texte indiqué dans l'image.
8. Cliquez sur **Terminer**.

Une fois vos informations correctement authentifiées, vous recevrez un e-mail contenant un URL d'activation. Cliquez sur l'URL pour activer votre nouveau mot de passe. Connectez-vous à la console Web EUQ à l'aide du mot de passe choisi à l'*Étape 5*.

Connexion à Hosted Email Security Web End-User Quarantine

Après avoir créé un nouveau compte, vous recevrez un e-mail indiquant que vos informations ont été authentifiées et que votre compte a été créé.

Pour vous connecter à Web End-User Quarantine pour la première fois :

1. Ouvrez le message reçu confirmant que votre compte a été créé.
2. Cliquez sur le lien sous forme d'URL d'activation.

   L'écran de connexion à Web EUQ s'affiche comme indiqué à la *figure C-2*.
3. Entrez l'adresse électronique utilisée pour configurer le compte.
4. Entrez le mot de passe choisi lors de la création du compte.
5. Cliquez sur **Connexion**.

Traitement des spams en quarantaine

L'écran Spams mis en quarantaine est le premier écran qui s'affiche lors de votre connexion à Web EUQ. Sur cet écran, vous pouvez :

- Afficher et trier la liste des messages en quarantaine dont l'accès à votre boîte de réception a été refusé
- Exécuter une action parmi les trois actions optionnelles à l'encontre de vos messages mis en quarantaine :
  - Supprimer
  - Transmettre (Non spam)
  - Transmettre et approuver l'expéditeur

L'écran des spams mis en quarantaine affiche, au-dessus du tableau, le nombre d'adresses d'expéditeurs actuellement approuvés. Consultez la section *Utilisation de l'écran Expéditeurs approuvés* à la page C-6 pour savoir comment ajouter ou modifier des adresses d'expéditeurs approuvés.

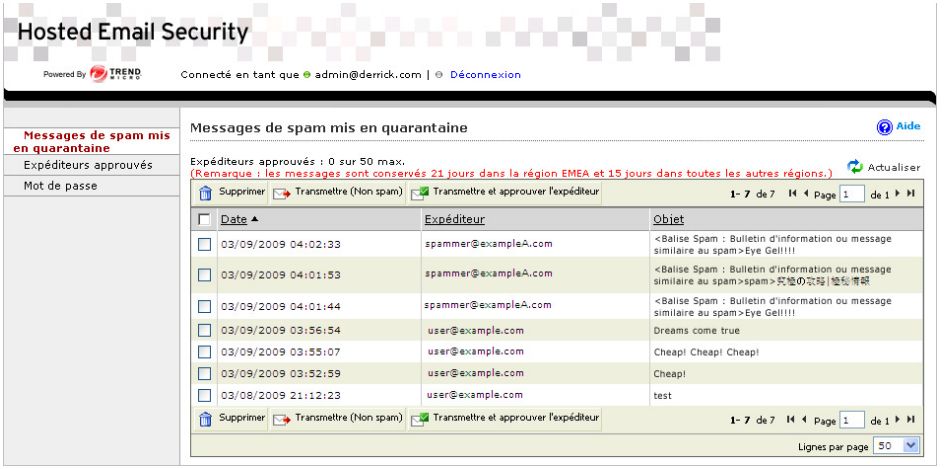


FIGURE C-4. Écran des spams mis en quarantaine

Pour afficher et trier dans le tableau les éléments en quarantaine :

1. Le cas échéant, choisissez le nombre d'entrées de messages affichés (10, 25, 50, 100, 250, 500) à l'aide de la liste déroulante dans l'angle inférieur droit du tableau.
2. Passez d'une entrée de message à une autre en cliquant sur les images figurant à droite de la ligne d'en-tête :
   - |< première page
   - < page précédente
   - > page suivante
   - |> dernière page
3. Triez les entrées de message par ordre croissant ou décroissant dans les catégories suivantes :
   - heure et date de réception (mm/jj/aa, hh:mm:ss)
   - adresse d'expéditeur.
   - Objet

Pour exécuter l'une des trois actions à l'encontre des éléments en quarantaine :

1. Sélectionnez le ou les messages concernés en procédant de l'une des manières suivantes :
   - Cochez les cases à gauche de chaque entrée.
   - Cochez la case à gauche de l'en-tête de la colonne « Date » pour sélectionner tous les messages sur la page actuellement affichée.
2. Sélectionnez une action à exécuter :
   - **Supprimer ( ) :** le ou les messages sélectionnés sont supprimés.
   - **Transmettre (Non spam) ( ) :** le ou les messages sélectionnés sont envoyés à votre compte de messagerie.
   - **Transmettre et approuver l'expéditeur ( ) :** le ou les messages sélectionnés sont envoyés à votre compte de messagerie et les adresses des expéditeurs sont ajoutées à votre liste d'expéditeurs approuvés.

Remarque : Trend Micro Hosted Email Security conserve les messages mis en quarantaine pendant 21 jours au maximum dans la région EMEA et pendant 15 jours dans toutes les autres régions. Ces messages sont ensuite supprimés.

Utilisation de l'écran Expéditeurs approuvés

Dans l'écran Expéditeurs approuvés, vous pouvez :

- afficher une liste d'expéditeurs approuvés et trier ceux-ci par date d'approbation ou par adresse d'expéditeur ;
- approuver des adresses ou domaines spécifiques pouvant envoyer des e-mails à votre adresse de messagerie ;
- supprimer des adresses ou domaines d'expéditeurs approuvés existants ;
- modifier des adresses ou domaines d'expéditeurs approuvés existants.

Lors de l'utilisation de l'écran Expéditeurs approuvés, les conditions suivantes s'appliquent :

- Hosted Email Security permet d'enregistrer un maximum de 50 expéditeurs approuvés dans la liste.
- Les services de réputation de messagerie (Email Reputation Services ou ERS) ne bloquent aucun message provenant des expéditeurs (ou domaines) spécifiés.
- Les règles heuristiques antispam basées sur le contenu ne s'appliquent pas aux messages électroniques envoyés par les expéditeurs ou domaines spécifiés.
- Toutes les règles antivirus, basées sur le contenu et relatives aux pièces jointes, définies par votre administrateur, continuent de s'appliquer.

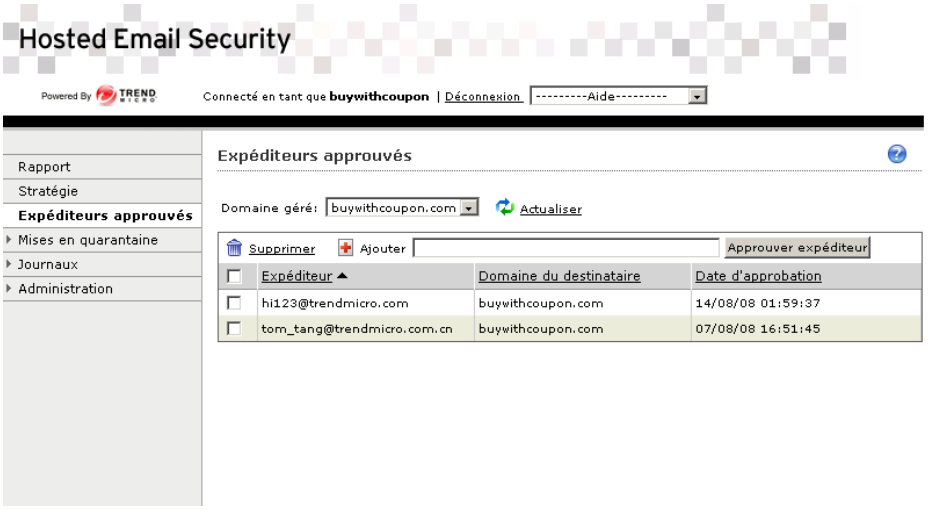


FIGURE C-5. Modification d'une adresse dans l'écran Expéditeurs approuvés

Tri des entrées de messages

Vous pouvez afficher les expéditeurs approuvés existants dans l'ordre croissant ou décroissant par :

- heure et date d'approbation (mm/jj/aa, hh:mm:ss) ;
- adresse d'expéditeur.

Ajout ou modification d'expéditeurs approuvés

Pour ajouter un expéditeur approuvé :

1. Entrez une adresse ou un domaine unique dans le champ **Ajouter**.
   - Pour une seule adresse, utilisez le modèle suivant : nom@exemple.com
   - Pour un domaine, utilisez le modèle suivant : *@exemple.com

> **Remarque :** Le caractère générique * n'est accepté que s'il précède le signe « @ ». Les deux exemples ci-dessus constituent les seuls formats autorisés pour un expéditeur approuvé. *@* ou d'autres formats d'adresse ne sont pas acceptés.

2. Cliquez sur **Ajouter**.

Pour modifier des adresses ou domaines d'expéditeurs approuvés existants :

1. Cliquez sur le lien de l'adresse électronique à modifier.

   Un champ modifiable est créé.
2. Modifiez l'adresse ou le domaine.
3. Cliquez sur **Envoyer** pour enregistrer l'adresse ou le domaine modifié.

Modification du mot de passe

Trend Micro vous recommande de changer votre mot de passe régulièrement. En outre, Web End User Quarantine (EUQ) requiert un mot de passe de 8 à 32 caractères.

Web EUQ vous permet de modifier votre mot de passe de deux manières :

- *Pour modifier votre mot de passe lorsque vous le connaissez :*
- *Pour redéfinir votre mot de passe :*

Pour modifier votre mot de passe lorsque vous le connaissez :

1. Cliquez sur **Mot de passe** dans le menu de gauche.
2. Entrez vos mots de passe actuel et précédent.

> **Remarque :** Trend Micro vous recommande vivement d'utiliser des mots de passe contenant plusieurs types de caractères (combinaison de lettres, chiffres et caractères spéciaux).

3. Entrez et confirmez votre nouveau mot de passe.
4. Cliquez sur **Enregistrer**.

Pour redéfinir votre mot de passe Web EUQ, vous devez vous souvenir de la question de sécurité que vous avez choisie lors de la création de votre compte. Si vous ne vous souvenez plus de la question ni de la réponse, l'administrateur système de votre messagerie peut redéfinir votre mot de passe à votre place.

Pour redéfinir votre mot de passe :

1. Accédez à l'**écran de connexion** et cliquez sur le lien **Vous avez oublié votre mot de passe ?**.

   L'écran indiqué à la *figure C-6* s'affiche.

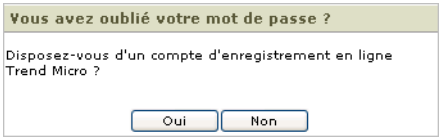


FIGURE C-6. Boîte de dialogue « Vous avez oublié votre mot de passe ? »

2. Si vous disposez d'un compte d'enregistrement en ligne (OLR) Trend Micro, cliquez sur **Oui**. Web EUQ vous redirige vers la page « Vous avez oublié votre mot de passe ? » sur le site OLR.
3. Si vous ne disposez pas d'un compte OLR, cliquez sur **Non**. L'écran indiqué à la figure C-7 à la page C10 s'affiche.

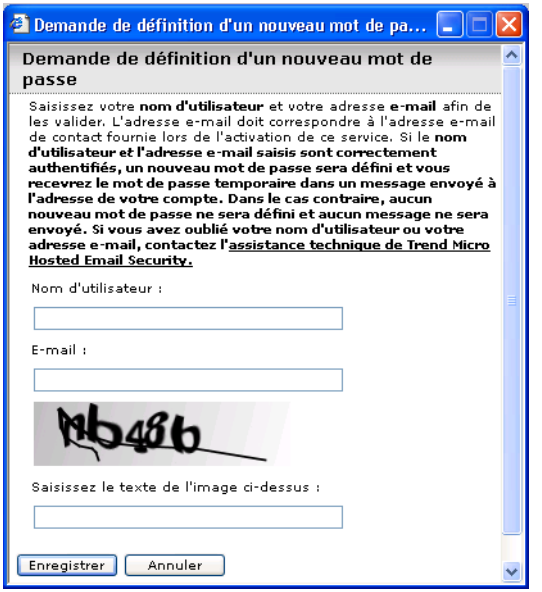

Demande de définition d'un nouveau mot de pa...
Demande de définition d'un nouveau mot de passe
Saisissez votre nom d'utilisateur et votre adresse e-mail afin de les valider. L'adresse e-mail doit correspondre à l'adresse e-mail de contact fournie lors de l'activation de ce service. Si le nom d'utilisateur et l'adresse e-mail saisis sont correctement authentifiés, un nouveau mot de passe sera défini et vous recevrez le mot de passe temporaire dans un message envoyé à l'adresse de votre compte. Dans le cas contraire, aucun nouveau mot de passe ne sera défini et aucun message ne sera envoyé. Si vous avez oublié votre nom d'utilisateur ou votre adresse e-mail, contactez l'assistance technique de Trend Micro Hosted Email Security.
Nom d'utilisateur :
E-mail :
Saisissez le texte de l'image ci-dessus :
Enregistrer
Annuler

FIGURE C-7. Écran Définition d'un nouveau mot de passe pour les utilisateurs ne disposant pas d'un compte OLR

4. Entrez vos nom d'utilisateur et mot de passe Hosted Email Security.

Remarque : L'adresse électronique doit correspondre à l'adresse électronique de contact fournie lors de l'activation du service.

---

5. Entrez le texte indiqué dans l'image de vérification CAPTCHA.
6. Cliquez sur **Enregistrer**. Une fois vos informations correctement authentifiées, vous recevrez un e-mail contenant un URL d'activation.
7. Cliquez sur l'URL d'activation contenu dans l'e-mail. Web EUQ active votre nouveau mot de passe et affiche une page de confirmation.

8. Dans la page de confirmation, cliquez sur **Continuer** et connectez-vous à la console Web EUQ à l'aide du mot de passe choisi à l'*Étape 5*.

Remarque : Si vos informations ne peuvent pas être authentifiées, le mot de passe ne sera pas redéfini. Si vous avez oublié l'adresse électronique ou la question de sécurité fournie au départ, contactez votre administrateur système. L'administrateur système peut redéfinir votre mot de passe à votre place.

Glossaire

Ce glossaire décrit les termes spécifiques utilisés dans ce document et dans l'aide en ligne.

TERME	EXPLICATION
action (*Voir également :* notification)	Opération devant être exécutée dans les situations suivantes : • un virus a été détecté • un spam a été détecté • une violation de contenu s'est produite • une tentative d'accès à un URL bloqué s'est produite, ou • le blocage d'un fichier a été déclenché Les actions les plus courantes sont les suivantes : Nettoyer et transmettre, Mettre en quarantaine, Supprimer et Transmettre/Transférer quand même. L'utilisation de l'action Transmettre/Transférer quand même n'est pas recommandée : l'envoi d'un message infecté ou le transfert d'un fichier infecté peut compromettre votre réseau.
activer	Activer votre logiciel au terme du processus d'enregistrement. Les produits Trend Micro ne fonctionnent pas tant qu'ils ne sont pas activés. Activez votre produit avant ou après son installation, dans l'écran Licence de produit (dans la console d'administration).
administrateur	Désigne « l'administrateur système » : personne au sein de l'entreprise responsable des activités telles que l'installation des nouveaux matériels et logiciels, l'affectation des noms d'utilisateur et mots de passe, le suivi de l'espace disque disponible et des autres ressources informatiques, l'exécution des sauvegardes et la gestion de la sécurité du réseau.
adresse électronique de l'administrateur	Adresse utilisée par l'administrateur de votre produit Trend Micro pour la gestion des notifications et alertes.

TERME	EXPLICATION
aide en ligne	Documentation intégrée à l'interface graphique d'administration.
antivirus	Programme informatique conçu pour détecter et nettoyer les virus informatiques.
archive	Fichier contenant (généralement) un ou plusieurs autres fichiers, ainsi que des informations permettant de les extraire (séparément) à l'aide du programme approprié (par exemple, fichier .zip).
ATM (agent de transfert de messages)	Programme chargé de la remise des messages électroniques. *Voir également :* serveur SMTP.
attaque par refus de service (Denial of Service, DOS)	Messages électroniques adressés en groupe et incluant des pièces jointes volumineuses qui saturent les ressources de votre réseau jusqu'à ralentir (voire bloquer) le service de messagerie.
authentification	Vérification de l'identité d'une personne ou d'un processus. L'authentification permet de s'assurer que les transmissions de données numériques parviennent au bon destinataire. Pour le destinataire, l'authentification constitue également une garantie d'intégrité du message et de sa source (origine ou expéditeur). La forme d'authentification la plus simple requiert un nom d'utilisateur et un mot de passe pour accéder à un compte particulier. Les protocoles d'authentification peuvent également utiliser le chiffrement à clé secrète (par exemple, algorithme Data Encryption Standard (DES)) ou les systèmes à clé publique qui utilisent des signatures numériques. *Voir également :* chiffrement à clé publique *et* signature numérique.
bloquer	Empêcher les intrusions dans votre réseau.

TERME	EXPLICATION
charge	Action d'un virus sur un ordinateur infecté. Celle-ci peut être relativement inoffensive (affichage de messages ou éjection du lecteur de CD) ou destructrice (suppression de l'ensemble des données d'un disque dur).
chiffrement	Processus de transformation des données dans un format qui ne peut être lu que par le destinataire légitime. Pour déchiffrer le message, le destinataire doit disposer de la clé de déchiffrement appropriée. Dans les schémas de chiffrement classiques, l'expéditeur et le destinataire utilisent la même clé pour chiffrer et déchiffrer les données. Les schémas de chiffrement à clé publique utilisent deux clés : une clé publique, que chacun peut utiliser, et une clé privée correspondante, détenue uniquement par la personne qui l'a créée. Grâce à cette méthode, un utilisateur quelconque peut envoyer un message chiffré à l'aide de la clé publique d'un propriétaire. Ce dernier est le seul à disposer de la clé privée permettant de déchiffrer le message. Les schémas de chiffrement à clé publique les plus courants sont PGP (Pretty Good Privacy) et DES (Data Encryption Standard).
chiffrement à clé publique	Schéma de chiffrement dans lequel chaque utilisateur dispose d'une paire de « clés » appelées clé publique et clé privée. La clé publique de chaque utilisateur est publiée tandis que la clé privée reste secrète. Les messages sont chiffrés à l'aide de la clé publique du destinataire et ne peuvent être déchiffrés qu'à l'aide de sa clé privée. *Voir également :* authentification *et* signature numérique.
clé d'enregistrement	Code à 22 caractères (tirets compris) utilisé dans certaines régions pour l'enregistrement dans la base de données client de Trend Micro. Voici un exemple de clé d'enregistrement : SM-27RT-UY4Z-39HB-MNW8 *Voir également :* code d'activation.

TERME	EXPLICATION
client	Système ou processus informatique qui utilise un protocole pour demander un service à un autre système ou processus informatique (« serveur ») et accepter les réponses du serveur. Un client fait partie d'une architecture logicielle client-serveur.
code d'activation	Code à 37 caractères (tirets compris) utilisé pour l'activation des produits Trend Micro. Voici un exemple de code d'activation : SM-9UE7-HG5B3-8577B-TD5P4-Q2XT5-48PG4 *Voir également :* clé d'enregistrement.
compte administrateur	Nom d'utilisateur et mot de passe associés à des privilèges d'administrateur.
configuration	Sélection d'options permettant de définir le fonctionnement de votre produit Trend Micro (par exemple, sélection de la mise en quarantaine ou de la suppression des messages infectés par un virus).
console de gestion	Interface utilisateur de votre produit ou service Trend Micro.
contrat de licence d'utilisateur final	Contrat légal passé entre un éditeur de logiciel et un utilisateur. Il souligne généralement les restrictions s'appliquant à l'utilisateur, qui peut refuser de valider l'accord en ne cliquant pas sur « J'accepte » lors de l'installation. La sélection de l'option « Je n'accepte pas » arrête l'installation du logiciel. En acceptant le contrat de licence d'utilisateur final affiché lors de l'installation de certains logiciels libres, de nombreux utilisateurs autorisent sans le savoir l'installation de spywares et programmes publicitaires sur leur ordinateur.

TERME	EXPLICATION
déclencheur	Événement provoquant l'exécution d'une action. Par exemple, votre produit Trend Micro détecte un virus dans un message électronique. Cette détection peut *entraîner* le placement du message en quarantaine et l'envoi d'une notification à l'administrateur système, à l'expéditeur du message et à son destinataire par le produit ou le service.
déroutement SNMP	Mécanisme de programmation qui gère les erreurs et autres problèmes d'un programme informatique. Un déroutement SNMP gère les erreurs relatives à la surveillance des périphériques réseau. *Voir :* SNMP.
DNS	Domain Name System (système de nom de domaine). Service de demande de données principalement utilisé sur Internet pour convertir les noms d'hôte en adresses IP.
domaine (d'administration)	Groupe d'ordinateurs doté d'une base de données et d'une stratégie de sécurité communes.
en-tête (définition du réseau)	Portion d'un paquet de données contenant des informations transparentes sur le fichier ou la transmission.
enregistrement	Processus d'identification en tant que client Trend Micro (à l'aide d'une clé d'enregistrement de produit dans certaines régions) dans l'écran d'enregistrement en ligne Trend Micro. https://olr.trendmicro.com/registration
entrant	Messages électroniques ou autres types de données acheminées vers votre réseau.

TERME	EXPLICATION
Ethernet	Technologie de réseau local (Local Area Network, LAN) développée par Xerox Corporation (centre de recherche de Palo Alto). Ethernet est un système de transmission performant utilisant la technologie CSMA/CD. Ethernet peut être utilisé avec différents schémas de câblage (câble 10Base5, câble 10Base2, câble 10BaseT et câble à fibre optique). Il s'agit d'une norme pour la connexion d'ordinateurs au sein d'un réseau local. La forme d'Ethernet la plus répandue est appelée 10BaseT (vitesse de transmission optimale de 10 Mbits/s avec un câble à paires torsadées en cuivre).
EUQ	Voir : *End User Quarantine*.
faux positif	Message électronique détecté par le filtre anti-spam et identifié comme spam par erreur.
fichier compressé	Fichier contenant un ou plusieurs autres fichiers, ainsi que des informations permettant de les extraire à l'aide du programme approprié (par exemple, fichier .zip).
fichier de signatures (Official Pattern Release, OPR)	Dernière compilation des signatures pour les menaces identifiées. Le fichier de signatures est soumis à divers tests approfondis pour assurer une protection optimale contre les dernières menaces. Il présente une efficacité accrue lorsqu'il est utilisé avec le dernier moteur de scan.
filtrage de contenu	Recherche dans les messages du contenu (mots ou phrases) enfreignant les stratégies de messagerie définies par le service informatique ou le service des ressources humaines de votre organisation (par exemple, contenus offensants, blasphématoires ou pornographiques).
filtrage sortant	Fonction optionnelle de Hosted Email Security qui filtre les spams dans le courrier sortant. Cette fonction doit être activée au préalable pour permettre l'activation du chiffrement d'e-mail.
hôte	Ordinateur connecté à un réseau.

TERME	EXPLICATION
HTTP	Hypertext Transfer Protocol : protocole TCP/IP client-serveur utilisé sur le Web pour l'échange de documents HTML. Par convention, il utilise le port 80.
HTTPS	Hypertext Transfer Protocol Secure : variante du protocole HTTP utilisée pour la gestion des transactions sécurisées.
Ko	Kilo-octet : 1 024 octets de mémoire.
LDAP (Lightweight Directory Access Protocol)	Protocole Internet que les programmes de messagerie utilisent pour localiser les informations de contact depuis un serveur. Par exemple, supposons que vous souhaitez localiser toutes les personnes à Boston disposant d'une adresse électronique contenant le prénom « Bob ». Une recherche LDAP vous permet de consulter les adresses électroniques correspondant à ce critère.
licence	Autorisation légale de faire usage d'un produit ou service Trend Micro.
liste des trous noirs en temps réel (RBL)	Liste d'adresses IP de serveurs de messagerie connus pour être des sources de spams.
liste dynamique des utilisateurs (DUL)	Associée à Trend Micro Email Reputation Services (ERS), cette liste contient les adresses IP attribuées dynamiquement, ou disposant de règles d'utilisation acceptables qui excluent les serveurs de messagerie publics.
Mo	Mégaoctet : 1 024 Ko de mémoire.
moteur de scan	Module exécutant le scan et la détection des menaces dans le produit hôte auquel il est intégré.
nettoyer	Supprimer un code de virus d'un fichier ou d'un message.

TERME	EXPLICATION
nom de domaine	Nom complet d'un système incluant son nom d'hôte local et son nom de domaine (par exemple, « tellsitall.com »). Le nom de domaine doit suffire pour déterminer l'adresse Internet unique d'un hôte sur Internet. Ce processus, appelé « résolution de nom », utilise le DNS.
notification (*Voir également :* action et cible)	Message transféré à un ou plusieurs des destinataires suivants : • administrateur système ; • expéditeur d'un message ; • destinataire d'un message ou d'un fichier (téléchargement ou transfert).
Open Proxy Stopper (OPS)	Associée à Trend Micro Email Reputation Services, cette liste contient les adresses IP des serveurs de proxy ouverts, connus pour avoir envoyé des spams.
pare-feu	Ordinateur passerelle sur lequel des mesures de sécurité spéciales sont définies, qui permet de servir des connexions réseau externes (notamment Internet) et des lignes entrantes.
passerelle	Interface entre une source d'informations et un serveur Web.
poste	Licence d'utilisation d'un produit Trend Micro destinée à une personne.
programme malveillant	Programmes ou fichiers développés dans le but de provoquer des dommages, tels que les virus, les vers et les chevaux de Troie.
programme publicitaire	Logiciel publicitaire qui affiche des bannières publicitaires pendant son exécution. Programme publicitaire installant une « porte dérobée ». Le mécanisme de suivi installé sur l'ordinateur de l'utilisateur à son insu est appelé « spyware ».

TERME	EXPLICATION
protocole Internet (Internet Protocol, IP)	Protocole Internet standard qui définit une unité de données appelée datagramme. Les datagrammes permettent de mettre en place un système de transmission performant, sans connexion. Le protocole Internet définit la transmission des informations entre les systèmes via Internet.
proxy	Processus fournissant un cache pour des éléments disponibles sur d'autres serveurs vraisemblablement plus lents ou plus difficiles d'accès.
QIL (Quick IP List)	Nom précédent de la base de données de réputation dynamique de Trend Micro Email Reputation Services.
Relay Spam Stopper (RSS)	Associée à Trend Micro Email Reputation Services, cette liste contient les adresses IP de serveurs de messagerie utilisés comme des relais ouverts, connus pour avoir envoyé des spams.
résolution DNS	Processus via lequel un client DNS demande le nom d'hôte et l'adresse d'un serveur DNS. Résultats de la configuration DNS de base sur un serveur exécutant une résolution par défaut. Par exemple, un serveur distant envoie une demande de données à un autre serveur concernant un ordinateur de la zone actuelle. Le logiciel client sur le serveur distant interroge le résolveur, qui répond à la demande à l'aide de ses fichiers de base de données.
routine des dommages	Partie destructrice d'un code de virus, également appelée charge.
RSS	Voir : *Relay Spam Stopper.*
scan basé sur les règles heuristiques	Scan du trafic réseau à l'aide d'une analyse logique des propriétés réduisant ou limitant la recherche de solutions.

TERME	EXPLICATION
serveur proxy	Serveur Web acceptant les URL utilisant un préfixe spécifique, utilisé pour rechercher des documents depuis un cache local ou un serveur distant, qui renvoie l'URL au demandeur.
serveur SMTP	Serveur relayant les messages électroniques vers leurs destinations.
signature numérique	Données supplémentaires ajoutées à un message qui identifient et authentifient l'expéditeur et les données du message à l'aide d'une technique appelée « chiffrement à clé publique ». *Voir également :* chiffrement à clé publique *et* authentification.
SMTP	Simple Mail Transfer Protocol : protocole utilisé pour le transfert de messages électroniques entre des ordinateurs (habituellement via Ethernet). Il s'agit d'un protocole entre serveurs, de sorte que d'autres protocoles sont utilisés pour accéder aux messages.
SNMP	Simple Network Management Protocol : protocole qui prend en charge la surveillance des périphériques associés à un réseau et recherche les conditions nécessitant une action de l'administrateur.
sortant	Messages électroniques ou autres types de données acheminées *hors* de votre réseau, vers Internet.
spyware	Logiciel publicitaire qui installe généralement un logiciel de suivi sur votre système et peut envoyer des informations vous concernant à un tiers. Le risque est que les utilisateurs ne puissent pas contrôler la nature des données collectées et leur utilisation.

TERME	EXPLICATION
stratégies	Offrent les mécanismes initiaux de protection du pare-feu pour vous permettre d'identifier le trafic qui y transite, en fonction des informations de la session IP. Elles protègent un réseau approuvé des attaques externes, telles que le scan de serveurs approuvés. Les stratégies créent un environnement dans lequel définir des stratégies de sécurité pour surveiller le trafic qui tente de franchir votre pare-feu.
type de fichier	Type de données stockées dans un fichier. La plupart des systèmes d'exploitation utilisent l'extension du nom de fichier pour déterminer son type. Le type de fichier permet de sélectionner l'icône appropriée pour représenter le fichier dans l'interface utilisateur, ainsi que l'application à utiliser pour l'afficher, le modifier, l'exécuter ou l'imprimer.
violation de contenu	Évènement ayant déclenché la stratégie de filtre de contenu.
virus	Programme (fragment de code exécutable) capable d'infecter un ordinateur. Comme les virus biologiques, il peut se répandre rapidement et est parfois difficile à éradiquer. Outre leur capacité de réplication, certains virus informatiques présentent une caractéristique commune : la routine des dommages qui déclenche la charge du virus. Si les charges peuvent simplement afficher des messages ou des images, elles peuvent également détruire des fichiers, reformater votre disque dur ou provoquer d'autres dommages. Même si le virus n'inclut pas de routine des dommages, il peut mobiliser de l'espace disque et de la mémoire et dégrader les performances de votre ordinateur.
Web End User Quarantine (EUQ)	Également appelé Web EUQ. Interface Web qui permet aux utilisateurs finaux de gérer les spams mis en quarantaine.
Web EUQ	Voir : *End User Quarantine*.

TERME	EXPLICATION
zone	Peut être un segment d'espace réseau auquel s'appliquent des mesures de sécurité (zone de sécurité), un segment logique auquel est liée une interface de tunnel VPN (zone de tunnel) ou une entité physique ou logique qui exécute une fonction spécifique (zone de fonction).

Index

Symboles

% de messages bloqués 2-14—2-15

A

acheter Email Encryption 2-8
action de rčgle
  contourner une rčgle 3-20
  rejeter un message 3-20
action en ligne 4-8, 4-10, 4-12
activation 2-3
Activation de règles 3-3
activation du service Email Encryption 2-6
active 5-35
Administration 5-11
administration des stratégies 3-2
  Liste de règles 3-3
Adresse IP de Hosted Email Security 1-3
adresses IP A-3
agent de transfert de messages 2-6
aide en ligne 2-11
Ajout d'une nouvelle règle 3-28
ajustements du moteur de scan B-7
aperçu des spams 4-4, 4-6—4-12
  action en ligne 4-10
  approbation des expéditeurs ou des messages 4-8, 4-12
  configuration minimale requise 4-11
  texte brut 4-9
aperçu, spam 4-4, 4-6—4-12
apprentissage par la machine 1-4
Assistance
  contacter B-2
  Ressources Internet B-1
Assistance technique
  contacter B-2
assistance technique par e-mail B-4
Assistant de transmission B-4—B-5
Attaque de type « Zip of Death » 3-4
Attaque par refus de service (Denial of Service, DOS) 3-4
Attaques de type DHA 5-13, A-1
Autres messages, nombre de champs (rapport de détail des menaces) 2-22
Avantages de Hosted Email Security A-1

B

Base de connaissances A-3, B-4

C

CAPTCHA C-10
Case Sensible à la casse, Ajouter une règle > écran Expressions à mot-clé, 3-12
Centre d'informations de sécurité B-7—B-8

Champ Bloqués dans le rapport de résumé des menaces 2-18
Champ Mis en quarantaine 2-16
Champ Non mis en quarantaine 2-16
Champ Sains dans le rapport de résumé des menaces 2-18
Champ Taille totale 2-16
Champ total des messages 2-15
Chiffrement d'e-mail
  action de règle 3-28
  configuration 3-21
  configuration requise 3-22
  déchiffrement 3-22
  lecture d'un e-mail chiffré 3-22, 3-25
  utilisation courante 3-21
Chiffrement, e-mail 3-21—3-22, 3-25, 3-28
chiffrement, e-mail 3-24
chiffrer des e-mails
  action de règle 3-21
Clé d'authentification de service 5-29—5-30
Clé d'enregistrement 2-9
Client Email Encryption 3-22
Clients des services Web 5-29
Code d'activation 2-4, 2-9
code de réponse 5-36
code suspect B-4
  comment soumettre B-6
comarquage 5-22
Confidentialité du service Hosted Email Security A-2
configuration
  agent de transfert de messages 2-6
configuration minimale requise 1-5
configurer le filtrage de contenu à l'aide d'expressions régulières 3-9
Configurer un message de notification 3-18
connexion 2-9
connexion à la messagerie, filtrage basé sur la réputation 1-4
Conservation des e-mails
  lorsque l'ATM est indisponible A-5
conservation des e-mails
  messages mis en quarantaine 4-6
Conservation des e-mails lorsque l'ATM est indisponible A-5
console d'administration 5-36, A-6
contacter
  informations générales B-3
contourner des rčgles 3-20
Copie d'une règle 3-38
couches de protection 1-4
Coût d'utilisation du service Trend Micro Hosted Email Security A-2
Curseur de réputation dynamique 5-3

D

date d'expiration 5-35
Déchiffrer l'e-mail 3-22
Délai de remise des e-mails A-4
déroulement des opérations 1-3
Désactivation de règles 3-3
désactivée 5-36
Destinataires de la notification 3-18
Détails des menaces
  tableau des totaux 2-22
Détails sur le suivi des messages 4-15
  accepté pour traitement 4-15

acceptés 4-15
bloqué ou retardé 4-15
non résolu 4-15
supprimé avec un virus 4-15
traité 4-15
transmis 4-15
DHA. Voir Attaques de type DHA.
disponibilité du service B-3

E

Ecran Ajouter des expressions à mot-clé 3-10
Écran d'un journal de suivi des messages 4-14
Écran des spams mis en quarantaine C-5
Ecran Expressions à mot-clé 3-7
Écran Expressions à mot-clé 3-9
Écran Gestion des répertoires 5-14
Écran Paramètres de réputation 5-2
e-mail
archivé A-4
chiffrement 3-21—3-22, 3-24—3-25, 3-28
connexion à la messagerie, filtrage basé sur la réputation 1-4
filtrage basé sur le contenu du message 1-4
retard A-4
stockage A-4
E-mail de notification
pour les actions Surveiller 3-27
E-mails archivés A-4
Encyclopédie des virus B-7
End User Quarantine
lien « Vous avez oublié votre mot de passe ? » 4-13
mot de passe réinitialisé par l'administrateur système de messagerie 4-13
enregistrement
clé d'enregistrement 2-2
enregistrement en ligne 2-9
Enregistrement Mail eXchange (MX) 1-3, 2-5, A-3
Enregistrement MX 1-3, 2-5, A-2
configuration 2-6
redirection A-3
envoi
message B-3
envoyer un e-mail à l'assistance technique B-4
ERS. Voir Services de réputation de messagerie (Email Reputation Services).
EUQ. Voir End User Quarantine.
évaluation
installation A-4
évaluations des risques B-8
expiration de la licence A-6
expiration totale 5-36
expirée 5-36
Exportation d'un fichier de répertoire d'utilisateurs 5-15
expression régulière 3-10
expressions à mot-clé
pondération 3-12
expressions régulières 3-9—3-10
filtrage de contenu avec 3-9
opérateurs disponibles 3-10
utilisation avec filtrage de contenu 3-9

F

Fichier de répertoire CSV 5-14
Fichier de répertoire d'utilisateurs
exportation 5-15
importation 5-15

fichier de test EICAR B-7
Fichiers compressés
  protégés par mot de passe 3-5
Fichiers compressés protégés par mot de passe 3-5
  pièces jointes 3-5
fichiers de signatures 1-4
fichiers suspects B-4
filtrage basé sur la réputation 1-4
filtrage basé sur la réputation au niveau de la connexion à la messagerie 1-4
filtrage basé sur le contenu du message 1-4
filtrage de contenu 1-4, 3-6
  avec des mots de passe 3-6
  expressions à mot-clé
    pondération 3-11—3-12
  expressions régulières 3-9
    sensibilité à la casse 3-11—3-12
  utilisation des expressions régulières 3-9
filtrage de contenu à l'aide des expressions régulières 3-9
Filtrage de niveau IP 5-7
filtrage sortant 2-6
  contacter Trend Micro pour obtenir 2-8
Flux de messages sortants A-5
flux des messages 1-3
Foire Aux Questions A-1
Foire aux questions A-1
fonctions propres à la version complète 1-2
Format LDIF 5-13

G

glossaire (Centre d'informations de sécurité) B-8
Guide de l'informatique sans risque B-7
Guide de l'utilisateur final Web EUQ 4-13

H

Hosted Email Security
  configuration minimale requise 1-5
Hosted Email Security (version complète)
  fonctions propres à 1-2

I

image CAPTCHA, avec service Email Encryption 3-25
Importation d'un fichier de répertoire d'utilisateurs 5-14—5-15
Importer répertoire d'utilisateurs 5-14
Indisponible
  Qu'arrive-t-il à mes messages si mon serveur de messagerie est indisponible pendant un certain temps ? A-5

J

journaux 4-14
  détails sur le suivi des messages 4-15

L

LDIF 5-13—5-14
lecture d'un e-mail chiffré 3-22
lien expressions à mot-clé 3-7, 3-22
limitations de scan
  action de rčgle 3-27
  contourner une rčgle 3-20
  rejeter un message 3-20
Liste d'expéditeurs approuvés 5-7
Liste d'expéditeurs bloqués 5-7
Liste de règles 3-3
livres blancs B-8
logo
  affichage de l'entreprise 5-23
  utilisation 5-22

M

Mail eXchange
  redirection A-3
maintenance B-3
maintenance du produit B-7
Menu Administration
  Modification du mot de passe 5-11
  stratégie 3-2
message
  envoi B-3
Message chiffré
  déchiffrement 3-22
  notification 3-23
Message de notification
  joindre une copie de l'original à 3-19
  liste des variables 3-19
message de notification, configuration 3-18
message sain, nombre de 2-21
messages
  % bloqués 2-14—2-15
  acceptés 2-14—2-15
  bloqués 2-14, 2-18
  mis en quarantaine 2-16
  non mis en quarantaine 2-16
  phishing 2-18
  Qu'arrive-t-il à mes messages si mon serveur de messagerie est indisponible pendant un certain temps ? A-5
  sains 2-18
  spam 2-18
  taille totale 2-16
  total 2-15, 2-18
  virus 2-18
messages acceptés 2-14—2-15
messages bloqués
  pourcentage de 2-22
messages entrants 5-36
messages entrants, trafic bloqué 2-14
messages nettoyés, nombre de 2-22
messages sortants 2-14
messages sortants, trafic bloqué 2-14
mises à jour des fichiers de signatures de virus B-7
modes de licence 5-35, A-6
modification d'une règle 3-36
Modification d'une règle 3-28
modification du mot de passe 5-11
Mot de passe
  modification 2-10
mot de passe
  modification 5-11
  modification du mot de passe administrateur 5-12
  modification du mot de passe de l'utilisateur final (Web EUQ) 5-13
  réinitialisation du mot de passe de l'utilisateur final 5-13
mot-clé, utilisation avec filtrage de contenu 3-6

N

Navigateur requis C-2
niveau d'exclusion pour les serveurs de messagerie à volume élevé 5-5
Niveau revendeur 5-22
niveaux de protection 1-4
nom de domaine complet A-3
notification
  envoi uniquement à son propre domaine 3-19
notification d'e-mail chiffré 3-23

notifications
horodatage 5-36

O

Ordre d'exécution des règles 3-26
Ordre des règles, exécution 3-26
Outil LDIFDE 5-15
instructions d'utilisation 5-15

P

Paramètre d'exclusion IP 5-4
paramètres de réputation
dynamique 5-3
Paramètres de réputation dynamique 5-3
par défaut 5-4
Paramètres de service standard 5-5
paramètres de stratégie, réglages par défaut 3-3
paramètres par défaut 1-5
Paramètres, par défaut 1-5
pare-feu A-3
Passerelle
solutions de passerelle Internet A-2
Passerelle de messagerie sécurisée, fiabilité A-2
période de grâce 5-36, A-6
phishing 2-18
nombre (rapport de détail des menaces) 2-21
stratégie par défaut 3-4
pièce jointe à haut risque 3-5
pièce jointe, haut risque 3-5
Principaux destinataires de virus 2-26
Prix A-2

Q

QIL 5-9
Quarantaine 4-3
conservation des e-mails 4-6

R

Rapport de détail des menaces
autres messages, nombre d' 2-21
messages sains, nombre de 2-21
phishing, nombre de 2-21
spams, nombre de 2-21
tableau des totaux 2-22
total quotidien 2-22
virus, nombre de 2-21
Rapport de résumé sur les menaces 2-18
Champ Autres 2-18
Champ Bloqués 2-18
Champ Phishing 2-18
Champ Sains 2-18
Champ Virus 2-18
spam 2-18
total 2-18
Rapport de trafic total 2-13
Rapport des principaux destinataires de spams 2-25
rapport hebdomadaire sur les virus B-7
Rapport Taille acceptée
Champ Mis en quarantaine 2-16
Champ Non mis en quarantaine 2-16
Champ Taille totale 2-16
rapports
présentation 2-11
résumé des menaces 2-18
trafic bloqué 2-14
trafic total 2-13
RBL 5-8

Récupération après sinistre A-5
Redirection d'e-mails
e-mails, redirection A-3
Redirection MX A-3
Règles
activation/désactivation 3-3
ajout 3-28
copie 3-38
modification 3-28
ordre d'exécution 3-26
suppression 3-38
règles
modification 3-36
règles heuristiques 1-4
rejeter des messages 3-20
Remise des e-mails, délai nécessaire A-4
Répertoire d'utilisateurs
vérification 5-16
réputation d'URL 1-4
réseau de zombies 1-4
Ressources Internet B-1
retard A-4
RK. Voir clé d'enregistrement.
routage des e-mails par les serveurs Hosted Email Security 1-3
routage des messages par les serveurs Hosted Email Security 1-3

S

Section Répertoire d'utilisateurs importés 5-14
serveur Hosted Email Security
routage des e-mails 1-3
Serveurs de messagerie
Qu'arrive-t-il à mes messages si mon serveur de messagerie est indisponible pendant un certain temps ? A-5
serveurs de messagerie
à volume élevé 5-5
blocage des serveurs de messagerie à volume élevé 5-2
serveurs de messagerie à volume élevé
niveau d'exclusion 5-5
Service d'alerte antivirus B-8
Service Email Encryption 3-21, 3-28
accusé de réception d'un message chiffré 3-23
achat 2-8
activation 2-6
Bouton Open my email (Ouvrir l'e-mail) 3-24
CAPTCHA 3-25
composant supplémentaire 2-2
Service hébergé de sécurité de messagerie, avantages A-1
Services de réputation de messagerie (Email Reputation Services) 1-4
Services Web 5-29
site d'enregistrement en ligne 2-9
Site End User Quarantine 4-11
soumission de code suspect à Trend Micro B-4
spam 2-18
stratégies par défaut 3-4—3-5
spams, nombre de 2-21—2-22
Stocker les e-mails A-4
stratégie de marque 5-22
stratégies par défaut 3-3, 3-5
Bulletin d'information ou message similaire au spam 3-5
pièce jointe à haut risque 3-5
spam ou phishing 3-4

taille du message 3-4
virus
comportement d'envoi en masse 3-4
nettoyable 3-4
non nettoyable 3-4
suivi des messages 4-15
suivi des messages sortants 2-14, 4-14—4-15
Suppression d'une règle 3-38

T

tableau des totaux
autres messages, nombre d' 2-22
messages bloqués, nombre de 2-22
messages bloqués, pourcentage de 2-22
messages nettoyés, nombre de 2-22
phishing, nombre de 2-22
spams, nombre de 2-22
virus, nombre de 2-22
taille des messages, stratégie par défaut pour 3-4
taille du message, stratégie par défaut pour 3-4
Taux de détection des spams 5-7
temps d'arrêt B-3
Tour d'horizon des virus B-7
trafic bloqué, entrant et sortant 2-14
Trend Micro
informations de contact B-3
part de marche des solutions de passerelle Internet A-2
TrendLabs B-7

U

URL
Base de connaissances B-4
Centre d'informations de sécurité B-7
URL de la base de connaissances B-7

V

Vérification du répertoire d'utilisateurs 5-16
Version complète
fonctions de 1-2
virus 2-18
règle par défaut 3-4
Virus Doctor B-6
Virus Doctor Voir TrendLabs
Virus, nombre (rapport de détail des menaces) 2-22
virusresponse@trendmicro.com B-6

W

Web End User Quarantine. Voir Web EUQ.
Web EUQ 4-13, C-1, C-3—C-4
actions C-6
aide en ligne 4-13
connexion C-4
création d'un nouveau compte C-3
description détaillée C-1
écran de connexion C-2
Écran des spams mis en quarantaine C-4
écran Expéditeurs approuvés C-6—C-7
modification d'adresses ou de domaines d'expéditeurs approuvés existants C-8
modification du mot de passe C-8
service C-2

Z

zombie 1-4